



# Cyber Security for Europe

## D4.5

### Research and Development Roadmap 3

Document Identification	
Due date	31 <sup>st</sup> January 2022
Submission date	31 <sup>st</sup> January 2022
Revision	6.0

Related WP	WP4	Dissemination Level	Public
Lead Participant	FORTH	Lead Author	Evangelos Markatos (FORTH)
Contributing Beneficiaries	AIT, ATOS, BBVA, CNR, Dawex, DTU, ENG, FORTH, ISGS, JAMK KUL, NTNU, POLITO, SIE, SINTEF, TDL, UCY, UM, UMA, UMU, UNITN, UPRC	Related Deliverables	D4.1, D4.3, D4.4

**Abstract:**

This is the third and last of a sequence of three research and development roadmaps of the CyberSec4Europe project. The goal of this roadmap is to identify major research challenges in the verticals of the project, and to explain what is at stake and what can go wrong if problems are left unsolved. The verticals studied are: (i) Open Banking, (ii) Supply Chain Security Assurance, (iii) Privacy-Preserving Identity Management, (iv) Incident Reporting, (v) Maritime Transport, (vi) Medical Data Exchange, and (vii) Smart Cities. For each vertical we identify the research challenges that need to be addressed and group them according to time in three phases: short term (until the end of the project), medium term (until 2025 – Security 2025), and long term (until 2030 – Security 2030). To emphasise the European nature of these roadmaps, each vertical clearly demonstrates how it can contribute to emerging dimensions including (i) the **Climate Change Dimension**, (ii) the **Impact on Democracy**, and (iii) the new **EU Cybersecurity Strategy for the Digital Decade**.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929. This document and its content are the property of the CyberSec4Europe Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license to the document or its contents. This document and its contents are not to be used or treated in any manner inconsistent with the rights or interests of the CyberSec4Europe Consortium and are not to be disclosed externally without prior written consent from the CyberSec4Europe Partners. Each CyberSec4Europe Partner may use this document in conformity with the CyberSec4Europe Consortium Grant Agreement provisions and the Consortium Agreement.



The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. Anyone using the information does so at their own sole risk and liability.

## Executive Summary

In the context of the CyberSec4Europe project, we publish a yearly research and development roadmap. This is the final one. Unlike other similar road mapping activities, which may aim to cover all (or most) aspects of cybersecurity, our roadmaps aim to explore emerging threats and to prioritise research directions, mainly in the areas of the **seven verticals** that have been identified in the project: (i) open banking, (ii) supply-chain security assurance, (iii) privacy-preserving identity management, (iv) incident reporting, (v) maritime transport, (vi) medical data exchange, and (vii) smart cities. Our previous roadmaps (Deliverables D4.3 and D4.4) were published in 2020 and 2021 (resp.) and focused on landscaping the research areas of the verticals and establishing the most important priorities [Markatos 2020, Markatos 2021].

This document, the last roadmap in the series, focuses on

1. *updating the research priorities*, introducing any new research topics, and possibly readjusting the ranking of existing ones
2. providing an updated state of the art
3. explaining how the chosen research priorities interact with the emerging dimensions of European policies as they relate to:
  - **Climate Change**
  - the **Impact on Democracy**
  - the new **EU Cybersecurity Strategy for the Digital Decade**.

The result of this exercise is an update set of priorities described against the backdrop of the priorities of Europe. Some of the priorities identified and/or areas that need more attention include:

- **Open Banking:**
  - Mapping of stakeholder interaction in end-to-end Open Banking processing
  - Setting up and discontinuing business relationships
  - Cross-border cooperation under differing legislation and security controls
  - Convenient and Compliant Authentication
  - Real time Revocation of Right of Access
  - Corporate Open Banking Security
- **Supply chain security assurance:**
  - Detection and management of supply chain security risks
  - Security hardening of supply chain infrastructures, including cyber and physical systems
  - Security and privacy of supply chain information assets and goods
  - Management of the certification of supply partners
- **Privacy-Preserving Identity Management**
  - System-based credential hardening
  - Unlinkability and minimal disclosure
  - Distributed oblivious identity management
  - Privacy preservation in blockchain
  - Password-less authentication
  - GDPR and eIDAS impact on Identity Management
  - Identity Management Solutions for the IoT

- **Incident Reporting**
  - Lack of harmonization of procedures
  - Facilitate the collection and reporting of incident and/or data leaks
  - Promote a collaborative approach for sharing incident reports to increase risk quantification, mitigation and thus overall cyber resilience
- **Maritime Transport**
  - Early identification and assessment of risks, threats and attack paths for critical maritime systems
  - Security hardening of maritime infrastructures, including cyber and physical systems
  - Resilience of critical maritime systems
  - Maritime system communication security
  - Securing autonomous ships
- **Medical Data Exchange**
  - Mechanisms for preserving user data privacy
  - Trustworthiness on the data exchange platform
  - Accomplish regulation during the data sharing process
  - Data exchange platform user experience
- **Smart Cities**
  - Trusted Digital Platform
  - Cyber threat intelligence and analysis platform
  - Cyber competence and awareness program
  - Privacy by design
  - Cyber response and resilience
  - End user trusted data management
  - Interoperability between legacy and new systems
  - Cyber fault/failure detection and prevention
  - Logging and monitoring
  - Information security and operational security

## How to read this document

- To provide a uniform approach to the roadmap, each vertical is covered in one section. Sections are numbered from 3 to 9. In the interests of homogeneity, subsections are structured as follows:
  - Subsections<sup>1</sup> \*.1 provide the big picture of the vertical.
  - Subsections \*.2 provide an overview.
  - Subsections \*.3 describe what is at stake for each vertical.
  - Subsections \*.4 describe the attackers.
  - Subsections \*.5 describe major recent incidents in each area.
  - Subsections \*.6 focus on the research dimension and provide background information. More specifically:
    - Subsections \*.6.1 describe the state of the art for each vertical
    - Subsections \*.6.2 provide a SWOT analysis;
    - Subsections \*.6.3 explain how each vertical contributes to **European Digital Sovereignty**;
    - Subsections \*.6.4 describe the interactions with **COVID-19** and the **Public Health Dimension**;
    - Subsections \*.6.5 describe the interactions with the **Green Deal and Climate Change**;
    - Subsections \*.6.6 describe the impact on **Democracy**;
    - Subsections \*.6.7 describe the impact on the **EU Cybersecurity Strategy for the Digital Decade**;
    - Subsections 6.8 describe sector-specific dimensions (if any)
    - The remaining subsections of \*.6 summarize the above dimensions and describe the research challenges.
  - Subsections \*.7 describe the mapping of the challenges to the big picture.
  - Subsections \*.8 describe the methods and tools for the research challenges.
  - Subsections \*.9 provide the **roadmap** for each vertical. Each roadmap is structured in three phases:
    - Short-term, (until the end of the project);
    - **Security 2025** (until 2025); and
    - **Security 2030** (until 2030)
  - Finally, subsections \*.10 provide a **summary** of each vertical.

The reader who is familiar with D4.4 will realize that the structures of D4.5 and D4.4 are very similar, although new subsections have been provided to cover the emerging relevant dimensions, the major incidents and the new roadmap timeline.

To place this work in context, Section 10 provides progress with respect to work reported in the second Roadmap (D4.5 [Markatos 2021]). Finally, Section 11 surveys roadmaps (or similar research priorities documents) that were published in 2020 including:

- Concordia Roadmap (D4.4)

---

<sup>1</sup> The \* refers to the number of each main section, from 3 to 9. Thus \*.1 refers to subsections 3.1, 4.1, 5.1 etc. until subsection 9.1. Similarly, \*.2 means subsections 3.2, 4.2, 5.2, ... 9.2, and so on and so forth.

- Cyberwatching.eu EU Cybersecurity & Privacy Final Roadmap (D4.7)
- ECHO INTER-SECTOR CYBERSECURITY TECHNOLOGY ROADMAP (D4.3)
- ENISA CYBERSECURITY RESEARCH DIRECTIONS FOR THE EU'S DIGITAL STRATEGIC AUTONOMY
- ENISA THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS
- ENISA Threat Landscape 2021
- EU Security Union Strategy (COM(2020) 605 final)
- EU CyberSecurity Strategy for the Digital Decade (JOIN(2020) 18 final)
- EU Strategy to tackle Organised Crime 2021-2025 (SWD(2021) 74 final)
- Europol IOCTA
- EU Security Union Strategy (COM(2020) 605 final)
- EU CyberSecurity Strategy for the Digital Decade (JOIN(2020) 18 final)
- EU Strategy to tackle Organised Crime 2021-2025 (SWD(2021) 74 final)
- Europol IOCTA

We hope that this document will be a useful tool for people who are interested in studying and understanding (i) the importance and (ii) the European dimensions of the research challenges in the vertical areas of the project.

## Document information

### Contributors

<b>Name</b>	<b>Partner</b>
Cristina Alcaraz	UMA
Ahmad Amro	NTNU
Marco Angelini	ENG
Elias Athanasopoulos	UCY
Jorge Bernal	UMU
Karin Bernsmed	SINTEF
Panagiotis Bountakas	UPRC
Sunil Chaudhary	NTNU
Laura Colombini	ISGS
Said Daoudagh	CNR
Juan José Ortega Daza	UMA
Jérémy Decis	DAWEX
Christos Douligeris	UPRC
Jesús García	UMU
Vanesa Gil Laredo	BBVA
Vasileios Gkioulos	NTNU
David Goodman	TDL
Christos Grigoriadis	UPRC
Alba Hita	UMU
Marko Hölbl	UM
Wouter Joosen	KUL
Elma Kalogeraki	UPRC
Prabhakaran Kasinathan	SIE
Georgios Kavalieratos	NTNU
Marko Kompara	UM
Panagiotis Kotzanikolaou	UPRC
Stephan Krenn	AIT
Alberto Lluch Lafuente	DTU
Antonio Lioy	POLITO
Eda Marchetti	CNR
Evangelos Markatos	FORTH
Per Håkon Meland	SINTEF
Vincenzo Napolitano	ENG
Aida Omerovic	SINTEF
Jani Päijänen	JAMK
Spyros Papastergiou	UPRC
Ivan Pashchenko	UNITN
Juan Carlos Pérez Baún	Atos
Salvador Perez	UMU
Rodrigo Roman	UMA
Michael Salmony	TDL
Ernesto Pimentel Sánchez	UMA
Vincenzo Savarino	ENG

Antonio Skarmeta	UMU
Rafael Torres	UMU
Martin Wimmer	SIE
Ricarda Weber	SIE
Christos Xenakis	UPRC
Susana González Zarzosa	Atos

## Reviewers

Name	Partner
Elias Athanasopoulos	UCY
Sandro Luigi Fiore	UNITN
Javier Lopez	UMA
Kai Rannenberg	GUF
Ahad Niknia	GUF

## History

Version	Date	Authors	Comment
1	October 10 2021	Evangelos Markatos	Table of Contents
2	December 1 2021	All partners	First draft version
3	December 15 2021	All partners	First version to be sent for review by the Coordinator
4	December 20 2021	All partners	First version to be sent to the reviewers
5	January 14 2022	All partners	Second version to be sent to the reviewers
6	January 25 2022	All partners	Final version
6	January 31 2022	GUF	Final check, preparation and submission

---

## Short Table of Contents:

Executive Summary .....	iii
1 Introduction.....	1
2 Context and Methodology .....	3
3 Open Banking .....	13
4 Supply Chain Security Assurance.....	77
5 Privacy-Preserving Identity Management .....	125
6 Incident Reporting .....	161
7 Maritime Transport.....	200
8 Medical Data Exchange .....	262
9 Smart Cities.....	299
10 Progress since D4.4.....	355
11 Related Work.....	361
12 Summary .....	381
13 References.....	383

## Long Table of Contents:

Executive Summary .....	iii
How to read this document .....	v
1    Introduction.....	1
1.1    Connections with Deliverables D4.3 and D4.4 (Roadmaps 1 and 2).....	2
2    Context and Methodology .....	3
2.1    Methodology .....	3
2.1.1    What’s in it for Europe?.....	4
2.1.1.2    Interaction with important priorities .....	5
2.1.2    What is at stake?.....	7
2.1.3    Who are the attackers? .....	8
2.1.4    What can be done about it? .....	8
2.2    Summary of CyberSec4Europe Demonstration Cases.....	8
2.2.1    Open Banking.....	9
2.2.2    Supply Chain Security Assurance.....	9
2.2.3    Privacy-preserving identity management.....	10
2.2.4    Incident Reporting.....	10
2.2.5    Maritime Transport .....	10
2.2.6    Medical Data Exchange .....	11
2.2.7    Smart Cities.....	11
3    Open Banking .....	13
3.1    The Big Picture .....	13
3.1.1    RTS SCA.....	15
3.1.2    PSD2 and GDPR .....	15
3.1.3    European Data Strategy.....	17
3.1.4    Summary .....	18
3.2    Overview .....	18
3.3    What is at stake?.....	19
3.3.1    What needs to be protected? .....	20
3.3.2    What could go wrong? .....	20
3.3.3    Social Engineering & Malware Attacks.....	20
3.3.4    Certificate Verification.....	21

3.3.5	GDPR & PSD2.....	21
3.3.6	APIs.....	22
3.3.7	Bank Administration.....	23
3.3.8	Circles of Trust.....	23
3.3.9	What is the worst thing that can happen?.....	24
3.4	Who are the attackers?.....	25
3.5	Major incidents in this vertical.....	26
3.5.1	Phishing.....	26
3.5.2	Decentralised Finance.....	26
3.5.3	Authorised Push Payment (APP).....	27
3.6	Research Challenges.....	28
3.6.1	State of the Art.....	28
3.6.1.1	Summary.....	28
3.6.1.2	The Bad News.....	29
3.6.1.3	The Good News.....	35
3.6.2	SWOT Analysis.....	40
3.6.2.1	Strengths.....	40
3.6.2.2	Weaknesses.....	41
3.6.2.3	Opportunities.....	41
3.6.2.4	Threats.....	42
3.6.3	European Digital Sovereignty.....	43
3.6.4	COVID-19 and Public Health Dimension.....	46
3.6.4.1	Opportunities.....	46
3.6.4.2	Threats.....	47
3.6.4.3	Beyond COVID – the public health dimension.....	49
3.6.5	Green Deal and Climate Change.....	50
3.6.5.1	My Carbon Action.....	51
3.6.5.2	Bank of the West.....	52
3.6.5.3	Visa.....	53
3.6.5.4	Lloyds.....	53
3.6.6	Impact on Democracy.....	53
3.6.6.1	Financial Inclusion.....	54

3.6.7	Contributions to the EU CyberSecurity Strategy for the Digital Decade .....	54
3.6.7.1	Resilient infrastructure and critical services .....	54
3.6.7.2	Building a European Cyber Shield.....	56
3.6.7.3	An ultra-secure communication infrastructure.....	56
3.6.7.4	Securing the next generation of broadband mobile networks.....	56
3.6.7.5	An Internet of Secure Things .....	56
3.6.7.6	Greater global Internet security.....	56
3.6.7.7	A reinforced presence in the technology supply chain .....	56
3.6.7.8	A Cyber-skilled EU workforce .....	56
3.6.7.9	EU leadership on standards, norms and frameworks in cyberspace .....	56
3.6.7.10	Cooperation with partners and the multi-stakeholder community .....	56
3.6.7.11	Strengthening global capacities to increase global resilience .....	57
3.6.8	Brexit Dimension .....	57
3.6.9	Sector-specific Dimensions.....	58
3.6.9.1	The United States .....	58
3.6.9.2	Asia .....	60
3.6.10	Summary of the dimensions and impact on the roadmap .....	62
3.6.11	Challenge 1: Mapping of stakeholder interaction in end-to-end Open Banking processing	62
3.6.12	Challenge 2: Setting up and discontinuing business relationships.....	63
3.6.13	Challenge 3: Cross-border cooperation under differing legislation and security controls...	63
3.6.14	Challenge 4: Convenient and Compliant Authentication.....	65
3.6.15	Challenge 5: Real time Revocation of Right of Access.....	66
3.6.16	Challenge 6: Corporate Open Banking Security.....	66
3.7	Mapping of the Challenges to the Big Picture .....	67
3.8	Methods, Mechanisms, and Tools.....	68
3.8.1	Challenge 1: Mapping of stakeholder interaction in end-to-end Open Banking processing	68
3.8.2	Challenge 2: Setting up and discontinuing business relationships.....	69
3.8.3	Challenge 3: Cross-border cooperation under differing legislation and security controls...	69
3.8.4	Challenge 4: Convenient and compliant authentication.....	70
3.8.5	Challenge 5: Real time revocation of right of access.....	71
3.8.6	Challenge 6: Corporate open banking security .....	71
3.9	Roadmap .....	73
3.9.1	Short-term plan.....	73

3.9.2	Beyond the end of the project plan .....	73
3.9.2.1	Security 2025 .....	73
3.9.2.2	Security 2030 .....	74
3.9.3	Milestones .....	74
3.10	Summary .....	75
4	Supply Chain Security Assurance.....	77
4.1	The Big Picture .....	77
4.2	Overview .....	77
4.3	What is at stake?.....	78
4.3.1	What needs to be protected? .....	78
4.3.2	What is expected to go wrong? .....	79
4.3.3	What is the worst thing that can happen?.....	80
4.4	Who are the attackers? .....	82
4.5	Major incidents in this vertical.....	83
4.6	Research Challenges .....	84
4.6.1	State of the Art .....	84
4.6.1.1	Supply chain risks, vulnerabilities and resilience .....	84
4.6.1.2	Attack prevention, detection and response in supply chains.....	86
4.6.1.3	Data sharing in supply chain ecosystems.....	89
4.6.1.4	Monitoring for compliance .....	91
4.6.1.5	Issues on the Software Supply Chain.....	94
4.6.2	SWOT Analysis .....	95
4.6.2.1	Strengths.....	96
4.6.2.2	Weaknesses .....	97
4.6.2.3	Opportunities.....	97
4.6.2.4	Threats.....	98
4.6.3	European Digital Sovereignty .....	99
4.6.4	COVID-19 and Public Health Dimension.....	99
4.6.5	Green Deal and Climate Change.....	102
4.6.6	Impact on Democracy .....	104
4.6.7	Contributions to the EU CyberSecurity Strategy for the Digital Decade .....	104
4.6.7.1	Resilient infrastructure and critical services .....	104

4.6.7.2	Building a European Cyber Shield.....	105
4.6.7.3	An ultra-secure communication infrastructure.....	105
4.6.7.4	Securing the next generation of broadband mobile networks .....	105
4.6.7.5	An Internet of Secure Things .....	105
4.6.7.6	Greater global Internet security.....	106
4.6.7.7	A reinforced presence in the technology supply chain .....	106
4.6.7.8	A Cyber-skilled EU workforce .....	106
4.6.7.9	EU leadership on standards, norms and frameworks in cyberspace .....	106
4.6.7.10	Cooperation with partners and the multi-stakeholder community .....	107
4.6.7.11	Strengthening global capacities to increase global resilience .....	107
4.6.8	Sector-specific Dimensions.....	107
4.6.9	Summary of the dimensions and impact on the Roadmap.....	107
4.6.10	Challenge 1: Detection and management of supply chain security risks.....	108
4.6.11	Challenge 2: Security hardening of supply chain infrastructures, including cyber and physical systems	110
4.6.12	Challenge 3: Security and privacy of supply chain information assets and goods .....	111
4.6.13	Challenge 4: Management of the certification of supply partners .....	113
4.7	Mapping of the Challenges to the Big Picture .....	114
4.8	Methods, Mechanisms, and Tools.....	115
4.8.1	Challenge 1: Risk management methodologies and frameworks .....	115
4.8.2	Challenge 2: Distributed detection, continuous monitoring and incident management ....	116
4.8.3	Challenge 3: Traceability, Shared Data Spaces .....	117
4.8.4	Challenge 4: Continuous Certification.....	118
4.9	Roadmap .....	119
4.9.1	Short-term plan.....	119
4.9.2	Beyond the end of the project plan .....	120
4.9.2.1	Security 2025 .....	120
4.9.2.2	Security 2030 .....	121
4.9.3	Milestones .....	122
4.10	Summary .....	122
5	Privacy-Preserving Identity Management .....	125
5.1	The Big Picture .....	125
5.2	Overview .....	125
5.3	What is at stake?.....	127

5.3.1	What needs to be protected? .....	127
5.3.2	What is expected to go wrong? .....	127
5.3.3	What is the worst thing that can happen?.....	129
5.4	Who are the attackers? .....	129
5.5	Major incidents in this vertical.....	130
5.6	Research Challenges .....	132
5.6.1	State of the Art .....	132
5.6.1.1	System-based credential hardening.....	132
5.6.1.2	Unlinkability and minimal disclosure .....	132
5.6.1.3	Distributed oblivious identity management .....	134
5.6.1.4	Privacy preservation in blockchain .....	134
5.6.1.5	Password-less authentication .....	135
5.6.1.6	GDPR and eIDAS impact interoperability.....	137
5.6.1.7	Identity Management Solutions for the IoT .....	138
5.6.2	SWOT Analysis .....	139
5.6.2.1	Strengths.....	139
5.6.2.2	Weaknesses .....	140
5.6.2.3	Opportunities.....	141
5.6.2.4	Threats.....	141
5.6.3	European Digital Sovereignty .....	141
5.6.4	COVID-19 and Public Health Dimension.....	142
5.6.5	Green Deal and Climate Change.....	143
5.6.6	Impact on Democracy .....	144
5.6.7	Contributions to the EU CyberSecurity Strategy for the Digital Decade .....	144
5.6.7.1	Resilient infrastructure and critical services .....	144
5.6.7.2	Building a European Cyber Shield.....	145
5.6.7.3	An ultra-secure communication infrastructure.....	145
5.6.7.4	Securing the next generation of broadband mobile networks .....	145
5.6.7.5	An Internet of Secure Things .....	145
5.6.7.6	Greater global Internet security.....	145
5.6.7.7	A reinforced presence in the technology supply chain .....	145
5.6.7.8	A cyber-skilled EU workforce .....	145

5.6.7.9	EU leadership on standards, norms and frameworks in cyberspace .....	145
5.6.7.10	Cooperation with partners and the multi-stakeholder community .....	145
5.6.7.11	Strengthening global capacities to increase global resilience .....	146
5.6.8	Sector-specific Dimensions.....	146
5.6.9	Summary of the dimensions and impact on the Roadmap.....	146
5.6.10	Challenge 1: System-based credential hardening .....	146
5.6.11	Challenge 2: Unlinkability and minimal disclosure.....	147
5.6.12	Challenge 3: Distributed oblivious identity management.....	148
5.6.13	Challenge 4: Privacy preservation in blockchain.....	149
5.6.14	Challenge 5: Password-less authentication .....	150
5.6.15	Challenge 6: GDPR and eIDAS impact on Identity Management.....	151
5.6.16	Challenge 7: Identity Management Solutions for the IoT.....	153
5.7	Mapping of the Challenges to the Big Picture .....	154
5.8	Methods, Mechanisms, and Tools.....	154
5.8.1	System-based credential hardening.....	154
5.8.2	Unlinkability and minimal disclosure .....	155
5.8.3	Distributed oblivious identity management .....	155
5.8.4	Privacy preservation in blockchain .....	155
5.8.5	Password-less authentication .....	155
5.8.6	GDPR guidelines and eIDAS interoperability .....	156
5.8.7	Identity Management Solutions for the IoT .....	156
5.9	Roadmap .....	157
5.9.1	Short-term plan.....	157
5.9.2	Beyond the end of the project plan .....	157
5.9.2.1	Security 2025 .....	157
5.9.2.2	Security 2030 .....	158
5.9.3	Milestones .....	159
5.10	Summary .....	159
6	Incident Reporting .....	161
6.1	The Big Picture .....	161
6.2	Overview .....	161
6.3	What is at stake?.....	162
6.3.1	What is the underlying need?.....	162
6.3.2	What is expected to go wrong? .....	165

6.3.3	What is the worst thing that can happen?.....	167
6.4	Who are the main stakeholders? .....	168
6.5	Major incidents in this vertical.....	170
6.6	Research Challenges .....	172
6.6.1	State of the Art .....	172
6.6.1.1	Security incident reporting.....	173
6.6.1.2	Risk assessment methodologies on incident reports .....	175
6.6.2	SWOT Analysis .....	177
6.6.2.1	Strengths.....	177
6.6.2.2	Weaknesses .....	178
6.6.2.3	Opportunities.....	179
6.6.2.4	Threats.....	180
6.6.3	European Digital Sovereignty .....	181
6.6.4	COVID-19 and Public Health Dimension.....	181
6.6.5	Green Deal and Climate Change.....	183
6.6.6	Impact on Democracy .....	184
6.6.7	Contributions to the EU CyberSecurity Strategy for the Digital Decade .....	185
6.6.7.1	Resilient infrastructure and critical services .....	185
6.6.7.2	Building a European Cyber Shield.....	186
6.6.7.3	An ultra-secure communication infrastructure.....	186
6.6.7.4	Securing the next generation of broadband mobile networks .....	186
6.6.7.5	An Internet of Secure Things .....	186
6.6.7.6	Greater global Internet security.....	186
6.6.7.7	A reinforced presence on the technology supply chain .....	186
6.6.7.8	A Cyber-skilled EU workforce .....	188
6.6.7.9	EU leadership on standards, norms and frameworks in cyberspace .....	188
6.6.7.10	Cooperation with partners and the multi-stakeholder community .....	188
6.6.7.11	Strengthening global capacities to increase global resilience .....	189
6.6.8	Sector-specific Dimensions.....	189
6.6.9	Summary of the dimensions and impact on the Roadmap.....	190
6.6.10	Challenge 1: Lack of harmonization of procedures .....	190
6.6.11	Challenge 2: Facilitate the collection and reporting of incident and/or data leaks .....	191

6.6.12	Challenge 3: Promote a collaborative approach for sharing incident reports to increase risk quantification, mitigation and thus overall cyber resilience .....	192
6.7	Mapping of the Challenges to the Big Picture .....	193
6.8	Methods, Mechanisms, and Tools.....	193
6.8.1	Incident Data Collection .....	194
6.8.2	Incident Impact Assessment (and transferability to other organization) .....	194
6.8.3	Incident Reporting.....	195
6.8.4	Collaborative incident sharing platform.....	195
6.9	Roadmap .....	196
6.9.1	Short-term plan.....	196
6.9.2	Beyond the end of the project plan .....	197
6.9.2.1	Security 2025 .....	197
6.9.2.2	Security 2030 .....	197
6.9.3	Milestones .....	197
6.10	Summary .....	198
7	Maritime Transport.....	200
7.1	The Big Picture .....	200
7.2	Overview.....	201
7.3	What is at stake?.....	202
7.3.1	What needs to be protected? .....	202
7.3.2	What is expected to go wrong? .....	205
7.3.3	What is the worst thing that can happen?.....	206
7.4	Who are the attackers?.....	206
7.4.1	Maritime Threat Agents .....	206
7.4.1.1	Agent: Activists.....	206
7.4.1.2	Agent: Competitor.....	206
7.4.1.3	Agent: Corrupt Government Official.....	207
7.4.1.4	Agent: Cyber Vandal.....	207
7.4.1.5	Agent: Data Miner/Thief.....	207
7.4.1.6	Agent: Employee, Disgruntled.....	207
7.4.1.7	Agent: Government Spy.....	207
7.4.1.8	Agent: Government Cyberwarrior .....	207
7.4.1.9	Agent: Internal Spy .....	207
7.4.1.10	Agent: Sensationalist/Irrational Individual .....	208

7.4.1.11	Agent: Terrorist.....	208
7.4.1.12	Agent: Mobster.....	208
7.4.1.13	Agent: Mobster.....	208
7.4.1.14	Agent: Mobster.....	208
7.4.1.15	Agent: Mobster.....	208
7.5	Major incidents in this vertical.....	209
7.6	Research Challenges .....	210
7.6.1	State of the Art .....	211
7.6.1.1	Legal and regulatory background.....	211
7.6.1.2	Risk assessment in the maritime transport sector .....	214
7.6.1.3	Security hardening for critical (maritime) systems.....	217
7.6.1.4	Maritime communication system security and trust infrastructures .....	222
7.6.1.5	Secure autonomous ships .....	226
7.6.1.6	Resilience in critical (maritime) infrastructures.....	229
7.6.2	SWOT Analysis .....	231
7.6.2.1	Strengths.....	231
7.6.2.2	Weaknesses .....	232
7.6.2.3	Opportunities.....	232
7.6.2.4	Threats.....	233
7.6.3	European Digital Sovereignty .....	233
7.6.4	COVID-19 and Public Health Dimension.....	234
7.6.5	Green Deal and Climate Change.....	235
7.6.6	Impact on Democracy .....	236
7.6.7	Contributions to the EU CyberSecurity Strategy for the Digital Decade .....	238
7.6.7.1	Resilient infrastructure and critical services .....	238
7.6.7.2	Building a European Cyber Shield.....	238
7.6.7.3	An ultra-secure communication infrastructure.....	240
7.6.7.4	Securing the next generation of broadband mobile networks .....	240
7.6.7.5	An Internet of Secure Things .....	241
7.6.7.6	Greater global Internet security.....	241
7.6.7.7	A reinforced presence on the technology supply chain .....	242
7.6.7.8	A Cyber-skilled EU workforce .....	242

7.6.7.9	EU leadership on standards, norms and frameworks in cyberspace .....	243
7.6.7.10	Cooperation with partners and the multi-stakeholder community .....	243
7.6.7.11	Strengthening global capacities to increase global resilience .....	244
7.6.8	Sector-specific Dimensions.....	245
7.6.9	Summary of the dimensions and impact on the Roadmap.....	246
7.6.10	Challenge 1: Early identification and assessment of risks, threats and attack paths for critical maritime systems.....	246
7.6.11	Challenge 2: Security hardening of maritime infrastructures, including cyber and physical systems	247
7.6.12	Challenge 3: Resilience of critical maritime systems .....	248
7.6.13	Challenge 4: Maritime system communication security .....	249
7.6.14	Challenge 5: Securing autonomous ships .....	250
7.7	Mapping of the Challenges to the Big Picture .....	252
7.8	Methods, Mechanisms, and Tools.....	252
7.8.1	Risk management and threat modelling methodologies for the Maritime Transport sector	252
7.8.2	Secure Autonomous Ships .....	253
7.8.3	Attack scenarios/simulation - security hardening .....	254
7.8.4	Secure Maritime Communications.....	255
7.8.5	Resilience .....	255
7.9	Roadmap .....	257
7.9.1	Short-term plan.....	257
7.9.2	Beyond the end of the project plan .....	258
7.9.2.1	Security 2025 .....	258
7.9.2.2	Security 2030 .....	258
7.9.3	Milestones .....	259
7.10	Summary .....	259
8	Medical Data Exchange.....	262
8.1	The Big Picture .....	262
8.2	Overview .....	262
8.3	What is at stake?.....	263
8.3.1	What needs to be protected? .....	263
8.3.2	What is expected to go wrong? .....	264
8.3.3	What is the worst thing that can happen?.....	265

8.4	Who are the attackers? .....	265
8.5	Major incidents in this vertical.....	266
8.6	Research Challenges .....	267
8.6.1	State of the Art .....	267
8.6.1.1	Identity management and eIDs.....	268
8.6.1.2	Medical data privacy .....	270
8.6.1.3	Legal and regulatory considerations .....	272
8.6.2	SWOT Analysis .....	273
8.6.2.1	Strengths.....	274
8.6.2.2	Weaknesses .....	275
8.6.2.3	Opportunities.....	275
8.6.2.4	Threats.....	275
8.6.3	European Digital Sovereignty .....	275
8.6.4	COVID-19 and Public Health Dimension.....	277
8.6.4.1	Medical Data Exchange demonstrator facing COVID-19 .....	277
8.6.4.2	Mobile contact tracing apps in Europe.....	278
8.6.5	Green Deal and Climate Change.....	282
8.6.6	Impact on Democracy .....	283
8.6.7	Contributions to the EU CyberSecurity Strategy for the Digital Decade .....	283
8.6.7.1	Resilient infrastructure and critical services .....	283
8.6.7.2	Building a European Cyber Shield.....	283
8.6.7.3	An ultra-secure communication infrastructure.....	284
8.6.7.4	Securing the next generation of broadband mobile networks .....	284
8.6.7.5	An Internet of Secure Things .....	285
8.6.7.6	Greater global Internet security.....	285
8.6.7.7	A reinforced presence in the technology supply chain .....	285
8.6.7.8	A Cyber-skilled EU workforce .....	285
8.6.7.9	EU leadership on standards, norms and frameworks in cyberspace .....	285
8.6.7.10	Cooperation with partners and the multi-stakeholder community .....	285
8.6.7.11	Strengthening global capacities to increase global resilience .....	285
8.6.8	Sector-specific Dimensions.....	285
8.6.9	Summary of the dimensions and impact on the Roadmap.....	286

8.6.10	Challenge 1: Security and privacy .....	286
8.6.11	Challenge 2: Mechanisms for preserving user data privacy .....	287
8.6.12	Challenge 3: Trustworthiness on the data exchange platform .....	288
8.6.13	Challenge 4: Accomplish regulation during the data sharing process .....	288
8.6.14	Challenge 5: Data exchange platform user experience .....	290
8.7	Mapping of the Challenges to the Big Picture .....	290
8.8	Methods, Mechanisms, and Tools.....	291
8.8.1	Challenge 1: Security tools .....	291
8.8.2	Challenge 2: Privacy-preserving assets.....	292
8.8.3	Challenge 3: Trust mechanisms .....	292
8.8.4	Challenge 4: Accomplish Regulations .....	292
8.8.5	Challenge 5: User Experience .....	293
8.9	Roadmap .....	294
8.9.1	Short-term plan.....	294
8.9.2	Beyond the end of the project plan .....	295
8.9.2.1	Security 2025 .....	295
	• Encouraging medical professionals to use encryption in healthcare; .....	295
8.9.2.2	Security 2030 .....	295
8.9.3	Milestones .....	296
8.10	Summary .....	297
9	Smart Cities.....	299
9.1	The Big Picture .....	299
9.2	Overview .....	300
9.3	What is at stake?.....	301
9.3.1	What needs to be protected? .....	301
9.3.2	What is expected to go wrong? .....	304
9.3.3	What is the worst thing that can happen?.....	307
9.4	Who are the attackers?.....	308
9.5	Major incidents in this vertical.....	309
9.6	Research Challenges .....	310
9.6.1	State of the Art .....	310
9.6.1.1	Secure Data Sharing.....	310
9.6.1.2	Cyber Risk Assessment.....	313
9.6.1.3	Social Engineering and Phishing .....	315

9.6.2	SWOT Analysis .....	317
9.6.2.1	Strengths.....	318
9.6.2.2	Weaknesses .....	319
9.6.2.3	Opportunities.....	320
9.6.2.4	Threats.....	320
9.6.3	European Digital Sovereignty .....	321
9.6.4	European Digital Sovereignty .....	321
9.6.5	COVID-19 and Public Health Dimension.....	321
9.6.6	Green Deal and Climate Change.....	322
9.6.7	Impact on Democracy .....	324
9.6.8	Contributions to the EU CyberSecurity Strategy for the Digital Decade .....	325
9.6.8.1	Resilient infrastructure and critical services .....	325
9.6.8.2	Building a European Cyber Shield.....	325
9.6.8.3	An ultra-secure communication infrastructure.....	326
9.6.8.4	Securing the next generation of broadband mobile networks .....	326
9.6.8.5	An Internet of Secure Things .....	326
9.6.8.6	Greater global Internet security.....	326
9.6.8.7	A reinforced presence in the technology supply chain .....	326
9.6.8.8	A Cyber-skilled EU workforce .....	326
9.6.8.9	EU leadership on standards, norms and frameworks in cyberspace .....	326
9.6.8.10	Cooperation with partners and the multi-stakeholder community .....	326
9.6.8.11	Strengthening global capacities to increase global resilience .....	326
9.6.9	Sector-specific Dimensions.....	327
9.6.10	Summary of the dimensions and impact on the Roadmap.....	327
9.6.11	Challenge 1: Trusted Digital Platform .....	327
9.6.12	Challenge 2: Cyber threat intelligence and analysis platform .....	328
9.6.13	Challenge 3: Cyber competence and awareness program.....	330
9.6.14	Challenge 4: Privacy by design.....	331
9.6.15	Challenge 5: Cyber response and resilience.....	333
9.6.16	Challenge 6: End user trusted data management .....	334
9.6.17	Challenge 7: Interoperability between legacy and new systems.....	336
9.6.18	Challenge 8: Cyber fault/failure detection and prevention .....	337

9.6.19	Challenge 9: Logging and monitoring .....	339
9.6.20	Challenge 10: Information security and operational security .....	341
9.7	Mapping of the Challenges to the Big Picture .....	343
9.8	Methods, Mechanisms, and Tools.....	344
9.8.1	Integrated Security Risk Framework .....	345
9.8.2	Cyber competences and awareness program.....	348
9.8.3	Privacy by design and end user trusted data management.....	349
9.9	Roadmap .....	351
9.9.1	Short-term plan until the end of the project .....	351
9.9.1.1	Cyber response and resilience & Cyber fault/failure detection and prevention.....	351
9.9.1.2	End user trusted data management.....	351
9.9.1.3	Interoperability between legacy and new systems .....	352
9.9.1.4	Logging and monitoring.....	352
9.9.2	Beyond the end of the project plan .....	352
9.9.2.1	Security 2025 .....	352
9.9.2.2	Security 2030 .....	353
9.9.3	Milestones .....	353
9.10	Summary .....	353
10	Progress since D4.4.....	355
10.1	Open Banking.....	355
10.2	Supply Chain Security Assurance.....	356
10.3	Privacy-preserving identity management.....	357
10.4	Incident Reporting.....	357
10.5	Maritime Transport .....	358
10.6	Medical Data Exchange .....	359
10.7	Smart Cities.....	359
11	Related Work.....	361
11.1	Concordia Roadmap (D4.4) .....	361
11.1.1	Threat Landscape .....	361
11.1.2	Research and Innovation .....	362
11.1.3	Education and Skills.....	362
11.1.3.1	Short term.....	362
11.1.3.2	Mid-Term .....	362
11.1.3.3	Long-Term Aims.....	362

11.1.4	Other Roadmaps.....	362
11.2	Cyberwatching.eu EU Cybersecurity & Privacy Final Roadmap (D4.7) .....	363
11.3	ECHO INTER-SECTOR CYBERSECURITY TECHNOLOGY ROADMAP (D4.3).....	364
11.4	ENISA CYBERSECURITY RESEARCH DIRECTIONS FOR THE EU’S DIGITAL STRATEGIC AUTONOMY .....	365
11.5	ENISA THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS.....	368
11.6	ENISA Threat Landscape 2021 .....	369
11.6.1	Most Important Threats.....	371
11.6.1.1	Ransomware.....	371
11.6.1.2	Malware.....	371
11.6.1.3	Cryptojacking.....	372
11.6.1.4	E-mail related threats .....	372
11.6.1.5	Threats against data.....	372
11.6.1.6	Threats against availability and integrity .....	372
11.6.1.7	Disinformation – misinformation.....	372
11.6.1.8	Non-malicious threats .....	372
11.6.2	Key Trends.....	373
11.7	EU Security Union Strategy (COM(2020) 605 final) .....	374
11.8	EU CyberSecurity Strategy for the Digital Decade (JOIN(2020) 18 final) .....	375
11.9	EU Strategy to tackle Organised Crime 2021-2025 (SWD(2021) 74 final) .....	376
11.10	Europol IOCTA.....	378
11.10.1	Crime-as-a-service .....	378
11.10.2	Advances in ransomware .....	379
11.10.3	Child Sexual Abuse Material (CSAM) .....	379
11.10.4	On-line fraud.....	379
11.10.5	Dark web.....	379
12	Summary.....	381
13	References.....	383

## List of Figures

Figure 1: Open Banking will change the way financial transactions are being carried out.....	9
Figure 2: Collecting and re-using medical data is expected to result in breakthroughs in medicine.....	11
Figure 3: A simple personal finance management model.....	14
Figure 4: Payment Initiation Service Provider (PISP) .....	15
Figure 5: Overview of elements of API scheme .....	38
Figure 6: Open Banking SWOT Summary .....	40
Figure 7: My Carbon Action in action .....	52
Figure 8: Supply Chain SWOT Summary .....	95
Figure 9: Privacy-Preserving Identity Management SWOT Summary .....	139
Figure 10: Graphical overview of the NIS Directive. Source: Incident notification for DSPs in the context of the NIS Directive .....	164
Figure 11: Incident Reporting SWOT Summary .....	177
Figure 12: The big picture of a resilient EU maritime transport ecosystem .....	201
Figure 13: The ENISA taxonomy for critical maritime assets (Source: [ENISA 2019]) .....	203
Figure 14: Context diagram for autonomous ship operation (Source: [RN 2017]) .....	204
Figure 15: The ENISA threat taxonomy for the maritime transport sector (Source: [ENISA 2019]) .....	205
Figure 16: Examples of maritime communication channels .....	223
Figure 17: Overview of the APS Context .....	224
Figure 18: On-board network architecture.....	224
Figure 19: Maritime Transport SWOT Summary.....	231
Figure 20: Medical Data Exchange SWOT .....	274
Figure 21: Stakeholders and services.....	300
Figure 22: IoT Assembly Taxonomy (Source [ENISA 2018]).....	303
Figure 23: Industry 4.0 Asset Taxonomy (Source: [ENISA 2018]) .....	304
Figure 24: IoT Threat Taxonomy (Source: [ENISA 2018]) .....	306
Figure 25: IoT Threats Impact .....	308
Figure 26: Intel Threats Identification .....	309
Figure 27: Smart Cities SWOT Summary .....	318
Figure 28: PDCA cycles for SC vertical .....	347

## List of Tables

Table 1: Open Banking global comparisons .....	44
Table 2: Challenges identified in the Open Banking vertical and tools needed to address them .....	71
Table 3: Challenges identified in the Supply Chain Vertical and Tools needed to address them .....	118
Table 4: Challenges identified in the Privacy-Preserving Identity Management Vertical and Tools needed to address them.....	156
Table 5: Challenges identified in the Incident Reporting Vertical and Tools needed to address them .....	196
Table 6: Challenges identified in the Maritime Transport Vertical and Tools needed to address them....	256
Table 7: Interoperability of mobile contact tracing apps in some EU Member States .....	278
Table 8: Interoperability of mobile contact tracing apps in some EU Member States .....	279
Table 9: Challenges identified in the Medical Data Exchange Vertical and Tools needed to address them .....	293
Table 10: Challenges identified in the Smart Cities Vertical and Tools needed to address them. ....	344

## List of Acronyms and Abbreviations

<i>A</i>	<b>ABC</b>	Attribute-Based Credentials	
	<b>ASC</b>	Autonomous Ship Controller	
	<b>AIS</b>	Automatic Identification System	
	<b>AISP</b>	Account Information Service Provider	
	<b>AMPQ</b>	Advanced Message Queueing Protocol	
	<b>API</b>	Application Program Interface	
	<b>APS</b>	Autonomous Passenger Ship	
	<b>ASLR</b>	Address Space Layout Randomization	
	<b>ASC</b>	Autonomous Ship Controller	
	<b>ASPSP</b>	Account Servicing Payment Service Provider	
<i>B</i>	<b>BIMCO</b>	Baltic and International Maritime Council	
<i>C</i>	<b>CA</b>	Certificate Authority	
	<b>CBRN</b>	Chemical, Biological, Radiological and Nuclear	
	<b>CC0</b>	Creative Commons No Rights Reserved Licence	
	<b>CCFG</b>	Contextual Control-Flow Graph (CCFG)	
	<b>CERT</b>	Cyber Emergency Response Team	
	<b>CE-S</b>	Cyber Enabled Ships	
	<b>CII</b>	Critical Information Infrastructure	
	<b>CIRAS</b>	Cybersecurity Incident Report and Analysis System	
	<b>CNIL</b>	Commission Nationale de l'informatique et des Libertés	
	<b>C-PAT</b>	Customs-Trade Partnership against Terrorism	
	<b>CPS</b>	Cyber Physical Systems	
	<b>CREST</b>	Cyber Security Incident Response Guide	
	<b>CS4E</b>	CyberSec4Europe	
	<b>CSI</b>	Container Security Initiative	
	<b>CTI</b>	Cyber Threat Intelligence	
	<b>CYSM</b>	Cyber/Physical Security Management Systems	
	<i>D</i>	<b>DEP</b>	Data Exchange Platform
		<b>DID</b>	Decentralized Identifier
<b>DIF</b>		Decentralized Identifier Foundation	
<b>DLT</b>		Distributed Ledger Technology	
<b>DPIA</b>		Data Privacy Impact Assessment	
<i>E</i>	<b>EEA</b>	European Economic Area	
	<b>EBA</b>	European Banking Authority	
	<b>ECDIS</b>	Electronic Chart Display and Information System	
	<b>ECISO</b>	European CyberSecurity Organisation	
	<b>EDI</b>	Electronic Data Interchange	

	<b>EDPB</b>	European Data Protection Board
	<b>EDPS</b>	European Data Protection Supervisor
	<b>EEA</b>	European Economic Area
	<b>eID</b>	electronic IDentity
	<b>eIDAS</b>	electronic IDentification, Authentication and trust Services
	<b>EIOPA</b>	European Insurance Occupational Pensions Authority
	<b>EMSA</b>	European Maritime Safety Agency
	<b>ER</b>	Evidential Reasoning
	<b>ENISA</b>	European Network and Information Security Agency
	<b>ESMA</b>	European Securities and Markets Authority
	<b>EUMSS</b>	EU Maritime Security Strategy
<i>F</i>	<b>FACT</b>	Failure Attack CounTermeasure
	<b>FFIEC</b>	Federal Financial Institutions Examination Council
	<b>FIDO</b>	Fast IDentity Online Alliance
	<b>FIDO UAF</b>	FIDO Universal Authentication Framework
	<b>FIDO U2F</b>	FIDO Universal 2 <sup>nd</sup> Factor
	<b>FMEA</b>	Failure Model and Effects Analysis
	<b>FSB</b>	Financial Stability Board
	<b>FS-ISAC</b>	Financial Service Information Sharing and Analysis Centre
<i>G</i>	<b>GDPR</b>	General Data Protection Regulation
	<b>GAFAM</b>	Google, Amazon, Facebook, Apple and Microsoft
	<b>GNSS</b>	Global Navigation Satellite System
<i>H</i>	<b>HEO</b>	High Elliptical Orbit
<i>I</i>	<b>IACS</b>	International Association for Classification Societies
	<b>IBAN</b>	International Bank Account Number
	<b>IaaS</b>	Infrastructure as a Service
	<b>ICS</b>	Industrial Control Systems
	<b>ICT</b>	Information and Communication Technologies
	<b>IDM</b>	Identity Management
	<b>IHR</b>	International Health Regulations
	<b>ILR</b>	Instruction Location Randomization
	<b>IMO</b>	International Maritime Organization
	<b>INTERTANKO</b>	International Association of Independent Tanker Owners
	<b>IoT</b>	Internet of Things
	<b>IIoT</b>	Industrial Internet of Things
	<b>IMO</b>	International Maritime Organization
	<b>ISO</b>	International Organization for Standardization
	<b>ISM</b>	International Safety Management
	<b>ISMS</b>	Information Security Management Systems

	<b>ITU</b>	International Telecommunication Union
<i>J</i>	<b>JNPT</b>	Jawaharlal Nehru Port Trust
	<b>JRC</b>	Joint Research Centre (of the European Commission)
<i>L</i>	<b>LEO</b>	Low Earth Orbit
	<b>LPA</b>	Local Public Administration
	<b>LRIT</b>	Long Range Identification and Tracking
<i>M</i>	<b>MARISA</b>	Maritime Integrated Surveillance Awareness
	<b>MAP</b>	Ship-to-Medical Aid Provider
	<b>MASS</b>	Maritime Autonomous Surface Ships
	<b>MEDUSA</b>	Multi-ordEr Dependency approaches for managing cascading effects in port's global sUPply chain and their integration in riSk Assessment frameworks
	<b>MITIGATE</b>	Multidimensional, IntegraTed, rIsk assessment framework and dynamic, collaborative risk manaGement tools for critical information infrAstrucTrurEs
	<b>MRCC</b>	Ship-to-Maritime Rescue Coordination Centre
	<b>MSC</b>	Mediterranean Shipping Company
	<b>MSRAM</b>	Maritime Security RiskAnalysis Model
<i>N</i>	<b>NFC</b>	Nera-Field Communication
	<b>NIS</b>	Network and Information Security
	<b>NISD</b>	Network and Information Security Directive
	<b>NIST</b>	National Institute of Standards and Technology
	<b>NI-ZKP</b>	Non-Interactive Zero-Knowledge Proof (of Knowledge)
<i>O</i>	<b>OSINT</b>	Open Source Intelligence
	<b>OT</b>	Operational Technologies
<i>P</i>	<b>PA</b>	Public Administration
	<b>p-ABC</b>	Privacy Attribute-Based Credential
	<b>PET</b>	Privacy Enhancing Technologies
	<b>PHA</b>	Preliminary Hazard Analysis
	<b>PISP</b>	Payment Initiation Services Provider
	<b>PKI</b>	Public Key Infrastructure
	<b>PLC</b>	Programmable Logic Controller
	<b>PSD2</b>	Payment Services Directive 2
	<b>PSP</b>	Payment Services Provider
	<b>PSU</b>	Payment Services User
	<b>PUF</b>	Physical/physically Unclonable Function
<i>R</i>	<b>RAN</b>	Radio Access Network
	<b>RBN</b>	Rule-based Bayesian Network
	<b>RBAC</b>	Role-based Access Control
	<b>RCC</b>	Ship-to-Remote Control Centre
	<b>RIF</b>	Risk Influencing Factor
	<b>RPN</b>	Risk Priority Number

	<b>RTK</b>	Real-Time Kinematic
	<b>RTS</b>	Regulatory Technical Standards
	<b>RTU</b>	Remote Terminal Unit
	<b>RFID</b>	Radio-Frequency IDentification
<i>S</i>	<b>SaaS</b>	Software as a Service
	<b>SAML</b>	Security Assertion Markup Language
	<b>SAR</b>	Ship-to-Search and Rescue
	<b>SAS</b>	Satellite Application Service
	<b>SC</b>	Smart City
	<b>SCA</b>	Strong Customer Authentication
	<b>SCADA</b>	Supervisory Control and Data Acquisition
	<b>SCRM</b>	Supply Chain Risk Management
	<b>SELP</b>	Socio Ethical Legal and Privacy
	<b>SIEM</b>	Security Information and Event Management
	<b>SIS</b>	Ship Information System
	<b>SME</b>	Small or Medium-sized Enterprise
	<b>SSM</b>	Six-Step-Model
	<b>SSO</b>	Single Sign-On
	<b>SWOT</b>	Strengths, Weaknesses, Opportunities and Threats
<i>T</i>	<b>TEE</b>	Trusted Execution Environment
	<b>TOS</b>	Terminal Operating System
	<b>TPM</b>	Trusted Platform Module
	<b>TPP</b>	Third Party Provider
<i>U</i>	<b>UAV</b>	Unnamed Aerial Vehicles
	<b>UFoIE</b>	Uncontrolled Flows of Information and Energy
	<b>UNCTAD</b>	United Nations Conference on Trade and Development
<i>V</i>	<b>VDES</b>	VHF Data Exchange System
<i>W</i>	<b>WLAN</b>	Wireless Local Area Network
	<b>WHO</b>	World Health Organisation
<i>X</i>	<b>XSS</b>	Cross Site Scripting



# 1 Introduction

Over the past few years we have seen several organisations produce research roadmaps (sometimes called also “research priority lists”) in the area of cybersecurity. For example, in its recently published annual Threat Landscape [ENISA 2021C], **ENISA** identifies threats, threat actors and attack techniques, as well as describing relevant mitigation measures. **Europol** also recently published the 2021 edition of its annual publication IOCTA (Internet Organized Threat Assessment), in which it lists the evolution of the threats in cybercrime [Europol 2021].

In the context of the CyberSec4Europe project, we also publish a yearly research and development roadmap. Unlike some of the other publications, which may aim to cover all aspects of cybersecurity, our roadmaps aim to explore emerging threats and prioritise research directions, mainly in the areas of the **seven verticals** that have been identified in the project: (i) open banking, (ii) supply-chain security assurance, (iii) privacy-preserving identity management, (iv) incident reporting, (v) maritime transport, (vi) medical data exchange, and (vii) smart cities. Our first roadmap (Deliverable D4.3) was published in 2020 and focused on landscaping the research areas of the verticals and establishing the most important priorities [Markatos 2020].

This roadmap (Deliverable D4.5), which is the third in the series, focuses on

- (i) *updating* the research priorities,
- (ii) explaining how we interact with important dimensions and policies including
  - a. ***Climate Change***
  - b. the ***Public Health*** and COVID-19 challenge, and
  - c. the ***EU Cybersecurity Strategy for the Digital Decade***
- (iii) explaining how the chosen research priorities map into the future:
  - a. *Security 2025*, and
  - b. *Security 2030*

The rest of this document is structured as follows: Section 2 provides context and methodology. Sections 3 to 9 present the context and the roadmaps of each individual vertical, as listed above. Section 10 presents the progress that has been made since the publication of our second roadmap, and section 11 presents related work: roadmaps and similar documents that have been published in 2021.<sup>2</sup> Such documents include Roadmaps published by fellow pilots, such as CONCORDIA (see section 11.1 in page 361) and ECHO

## VERTICAL AREAS

OPEN BANKING

SUPPLY-CHAIN SECURITY  
ASSURANCE

PRIVACY-PRESERVING  
IDENTITY MANAGEMENT

INCIDENT REPORTING

MARITIME TRANSPORT

MEDICAL DATA EXCHANGE

SMART CITIES

<sup>2</sup> Note that Roadmaps published before 2021 were included in the related work of Deliverables D4.3, and D4.4.

(see section 11.3 in page 364), roadmaps and studies published by ENISA (Sections 11.4 to 0), as well as other documents of strategic importance for the EU.

## **1.1 Connections with Deliverables D4.3 and D4.4 (Roadmaps 1 and 2)**

The project's third roadmap, as implemented in the current deliverable, D4.5, is carefully designed to be self-contained. Otherwise, this third roadmap, which is a natural progression of the first roadmap (D4.3 delivered in 2020) and the second roadmap (D4.4 delivered in 2021) would be hard to read. To assist the reader while stressing this natural progression, we have formatted the content of the earlier roadmaps in a lightly shaded background: e.g. shaded text is taken from D4.3 and D4.4 Therefore, readers familiar with deliverables D4.3 and D4.4 can easily skip the shaded sections, or use them as a back reference, while studying the new material in the non-shaded text.

## 2 Context and Methodology

### 2.1 Methodology

Each individual vertical demonstration use case creates a roadmap according to its own needs and priorities. We should emphasize, however, that the individual vertical roadmaps go well beyond the scope (in time and space) of the needs of the demonstrators in Work Package WP5 and deal with their topic from a broader view. In this way they will be useful not only to the CyberSec4Europe Partners, but also to the broader constituency.

In order to have some uniformity across the different roadmaps, a common structure was proposed that should be followed in all cases. That is, the roadmap of each vertical should adopt as far as possible the following approach:

- Introduction
  - **Big Picture:** What is the broad setting of the vertical?
  - Overview: What is the problem that this vertical addresses?
- **What is at stake?**
  - What needs to be protected?
  - What is expected to go wrong?
  - What is the worst thing that can happen?
- Who are the **attackers**?
- **Major incidents** in the area of this vertical
  - What were the major incidents during the past 20 years? Who was behind them? What was their cost?
- What are the **research challenges** in this area?
  - **State of the Art**
    - What has been done?
  - **SWOT Analysis**
    - What are the strengths, weaknesses, opportunities and threats in these areas? The analysis should be made from the point of view of the European Union.
  - **European Digital Sovereignty**
    - Does this area contribute to European Digital Sovereignty? If yes, how?
  - **COVID-19 and Public Health Dimension**
    - Is there an interaction between the research in this vertical and COVID-19? Or possibly between this vertical and the increasing trend towards working from home and operating remotely? Any other issues relating to public health? How does your vertical interact with general issues of public health? Future pandemics? other diseases?
  - **Green Deal and Climate Change**
    - What is the interaction of this area with the green dimension? Is there any contribution that can be made?
    - What is the interaction with climate change (fires, floods, weather, food security, green issues, etc.)?

- **Impact on Democracy**
    - What is the impact on democracy? Civil liberties? Instability? Disinformation? Terrorism? Hactivism? War?
  - Sector-specific dimensions
    - Is there interaction with any sector-specific dimension?
  - Contributions to the **EU CyberSecurity Strategy for the Digital Decade**
    - How does research in each vertical contributes to the EU Strategy?<sup>3</sup> Specific topics of the Strategy include:
      - Resilient infrastructure and critical services
      - Building a European Cyber Shield
      - An ultra-secure communications infrastructure
      - Securing the next generation of broadband mobile networks
      - An Internet of Secure Things
      - Greater global Internet security
      - A reinforced presence in the technology supply chain
      - A cyber-skilled EU workforce
      - EU leadership on standards, norms and frameworks in cyberspace
      - Cooperation with partners and the multi-stakeholder community
      - Strengthening global capacities to increase global resilience
- How do these research challenges map into the big picture?
  - How do they relate to the Methods, Mechanisms, and Tools identified in Work Package WP3 of this project?
  - What is the **Roadmap**?
    - Which of the challenges are **short-term** and which are **long-term**?

These are the main questions for each individual roadmap:

- What is at stake?
- Who are the attackers?
- With respect to research, what can be done about it?
- What's in it for Europe?

These questions are analysed in the following subsections.

### 2.1.1 What's in it for Europe?

Since this research is being carried out in a European context, it is important to analyse the context of the research being performed within the European Union, as well as the interaction between the research challenges and this context. Along these lines, we have identified the following dimensions:

<sup>3</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=EN>

### 2.1.1.1.1 SWOT Analysis

In this analysis we would like to understand how Europe is equipped to address this kind of research challenges. For example:

- What are the strengths of Europe in this area?
- Is it the people?
- Is it the legal/policy framework?
- Is it the availability of infrastructures?
- Is it funding?
- Is it something else?

In addition to the strengths, we would also like to identify the weaknesses, the opportunities, and finally the threats to this research in the context of the EU. Although the SWOT analysis will refer to the context of the European Union, in some cases this will just be the starting point and the analysis may also have to consider the global context, too. Indeed, although the strengths are primarily European, the weaknesses need to consider the international dimension, which may result in competition, fragmented legal frameworks, etc. Similarly, opportunities and threats may also be global.

### 2.1.1.2 Interaction with important priorities

In this section we would like to explore how these research challenges interact with important European dimensions. Since Europe is a complex state union, many dimensions that affect these research challenges can play a critical role. In this roadmap, we have selected three dimensions that we find critical, and we justify this for each dimension below. The selection was challenging, since anyone can find additional important directions, possibly aligned with their background. We opted in for a small set of dimensions, just three, so that the discussion focuses more on depth than on breadth. In addition, we focused on the three that are *timely important* (e.g. the COVID-19 dimension) and that we have, at least, a preliminary assessment. One can argue that there are other several and timely important dimensions, we feel that currently those three are the ones that we have a better assessment.

- **European Digital Sovereignty**
  - Over the past few years, there is an increasing movement towards achieving European sovereignty in the digital space. Citizens are losing control of their data and of their ability to make meaningful decisions in the online environment. To address this issue, the four pilot projects (CONCORDIA, CyberSec4Europe, ECHO, and SPARTA) explore the steps that need to be taken in order to restore European Sovereignty in cyberspace.<sup>4</sup> Against this background, support has been growing for a new policy approach designed to enhance Europe's strategic autonomy in the digital field.<sup>5</sup> In this setting we would like to understand:
    - How does each vertical contribute to achieving European Digital Sovereignty?

---

<sup>4</sup> <https://cybersec4europe.eu/convergence/roadmapping-focus-group/>

<sup>5</sup> [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS\\_BRI\(2020\)651992\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf)

- 
- How does the goal of European Digital Sovereignty impact the research that needs to be done in each vertical?
- **COVID-19 and public health**
    - Over the past few years we all came to embrace a new kind of normality: working from home, no travelling, very little contact with other people. COVID-19 quickly forced us to adapt to the new normal. In any case, there was no other choice: it was either this kind of normal, or illness with the possibility of death. In this process we realised that technology can quickly become a friend and an enemy at the same time. Indeed, when schools and offices were closed, technology enabled us to continue work and study from home. However, at the same time we realised that almost everything that we did had a digital dimension: there was no way to talk to friends without using some kind of computing device. Similarly, as shops were closed, there was no way to shop without going online. One might think that this is a temporary thing and that once COVID-19 dies out, things will get back to “normal”. Unfortunately, it is unclear whether this is the case. COVID-19 is only one of the issues related to “Public Health”. The cybersecurity implications of choices for COVID-19 and public health will need to be studied. For example,
      - What kind of research needs to be done in this vertical to address the impact of current (e.g. COVID-19) and future public health issues?
      - Public health concerns<sup>6</sup> may quickly impose unforeseen measures (such as lockdowns and mandatory data sharing). How does cybersecurity and privacy interact with such measures?
  - **The Green Deal Dimension and Climate Change**
    - It is widely acknowledged that climate change and environmental degradation are an existential threat to Europe and the world.<sup>7</sup> The European Green Deal provides an action plan to (i) boost the efficient use of resources by moving to a clean, circular economy, and (ii) restore biodiversity and cut pollution. At the same time, we are witnessing an ever-increasing deterioration of the Climate Crisis, which seems to affect several aspects of everyday life.
    - Several of the verticals have significant interactions with this dimension. In this section we would like to explore:
      - How can research in the area of the vertical contribute to the Green Deal?
      - How can cybersecurity and privacy reduce the impacts of the Climate Crisis?
  - **Impact on Democracy**
    - Cybersecurity attacks have traditionally focused on the market and the financial impact. However, over the past five years we have seen digital media being used to impact elections and to undermine democracy and our democratic values. For example, fake news has recently been used to steer people into the wrong choices. Thus, we would like to explore:
      - What is the interaction of this vertical with our democratic values?

---

<sup>6</sup> Over the past two years we saw that COVID-19 forced several countries to get into lockdowns and completely changed the way we work, shop, and socialize. Now we see that the COVID-19 pandemic has significantly involved with the Delta/Omicron variants, and may continue to evolve in the future. As a result, we cannot preclude that similar changes to our lives will also happen in the future.

<sup>7</sup> [https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_en)

- How can security and privacy research defend against attacks towards democracy?
- **The EU Cybersecurity Strategy for the Digital Decade**
  - Recently the EU published its cybersecurity strategy for the digital Decade.<sup>8</sup> This strategy, among other things, includes “Resilient infrastructure and critical services”, “Building a European Cyber Shield”, “An ultra-secure communication infrastructure”, “Securing the next generation of broadband mobile networks”, “An Internet of Secure Things”, “A reinforced presence in the technology supply chain”, “A cyber-skilled EU workforce”, “Strengthening global capacities to increase global resilience”, etc. We would like to understand how the research in our verticals can contribute to these aspects of the EU Cybersecurity Strategy.

### 2.1.2 What is at stake?

Although the scope of the problem and the answer to the question “What is at stake?” may be obvious to security researchers, it may be far from clear to people who have no background in cybersecurity. Indeed, people may head about cyberattacks, about botnets, about data leaks, but they may not know what impact these attacks may have in their everyday lives. To illustrate this point, let us consider the following example: over the past few years we have heard about leaks of customer data which were kept on line by well-known companies<sup>9</sup>. Thus, it is natural to wonder: What is the **impact** of these data leaks? Is it a **financial loss**? Is it **damage** to property? **Loss of life**? – all the above? None of the above? What?

As another example to illustrate the same point, let us assume that an SME (Small or Medium-sized Enterprise) stores all its data, including customer and financial data, on a local computer. If this computer is compromised, what would that mean for the SME? What would the impact be? Inconvenience? **Financial loss**? Loss of **reputation**? Loss of business? Could the SME even **go out of business**? What?

It is important to give clear answers to these types of questions, so that we can determine the importance of the area of research. To be able to draw the picture correctly, we will focus on the following sub-questions:

- What is expected to go wrong under **ordinary conditions**? For example, under ordinary conditions the compromised computer of the SME above may do little harm. System administrators will identify the problem, clean it up, and eventually return it to normal operation.
- What is at stake under a **worst-case scenario**? That is, if everything goes wrong, what is the worst thing that can happen? For example, in a worst-case scenario, a compromised computer may result in significant harm. If it remains undetected, it may also compromise other computers, perhaps deleting all their data, including even backup copies, and potentially leading the SME to a total loss of all its records. In such an eventuality, most SMEs would not be able to recover.

<sup>8</sup> <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN>

<sup>9</sup> <https://www.cnbc.com/2019/07/30/five-of-the-biggest-data-breaches-ever.html>

### 2.1.3 Who are the attackers?

It is important for us to understand **who** the attackers are, what their **motives** are, and what kind of **resources** (people, money) they have at their disposal. For example:

- **script kiddies** have practically no resources, have little expertise and, having made some fuss, will go away.
- **Opportunistic hackers** may also have limited resources, and so they may do some limited damage, resulting in limited financial loss.
- **Organized hackers**, especially those linked to organized crime, may have more resources (possibly of the order of tens of thousands of euros), and their actions may involve major financial raids that enable them to recoup their initial investment.
- **Terrorists** have many resources and do not care about financial gain.
- At the far end of the spectrum, **enemy countries** have vast resources (hundreds of millions, if not billions, of euros and thousands of people), may do major damage, can stay undetected for quite some time, and may possibly inflict major damage on entire infrastructures (electric power grids, hospitals, water supplies, food supply chain, etc.).

### 2.1.4 What can be done about it?

Since this is a research and development roadmap, we are focusing on what research can be carried out to address the problems, avoid the worst-case scenarios, and reduce to the bare minimum possible the impact of the average case. To place the work in the appropriate context, we may divide the research chronologically: immediate (next 12 months), short-term (until the end of the project) and long-term (after the end of the project).

## 2.2 Summary of CyberSec4Europe Demonstration Cases

In this section we summarize the demonstration cases of the CyberSec4Europe project. A thorough treatment of these demonstration cases can be found in Work Package WP5.

## 2.2.1 Open Banking



Figure 1: Open Banking will change the way financial transactions are being carried out<sup>10</sup>

Open banking (see Figure 1) is a new idea in the financial world that is changing the way financial transactions are carried out. The main idea behind open banking is that people can share their financial data with any entity they choose, including merchants. To date, most financial data has been held by banks and not shared with third parties, other than in a limited number of cases. Open banking provides a way for people to enable third parties to access their financial data. Although open banking is highly convenient for consumers and has resulted in new applications and business opportunities, it also entails security implications. For example, social engineering may trick people into revealing their data, malware may perform fraudulent transactions, while identity theft may result in significant financial losses.

The objective of this demonstration use case is to address the risks and vulnerabilities posed by social engineering and malware attacks when users are seeking to obtain account information, to provide protection for bank administration security policies while overcoming weaknesses in the design and/or implementation of APIs (Application Programming Interfaces) in use, and to prevent fraud and data loss during the access to and request for payment by third parties in an open banking environment.

## 2.2.2 Supply Chain Security Assurance

The development of secure solutions is extremely important and can be extremely challenging when based on insecure components. Likewise, building safe high-quality products on top of dubious or unsafe supply chains is nearly impossible. This demonstration case deals with the security of the supply chain, in particular the quality and integrity of parts and products. The main challenge of this demonstration case is to use protection mechanisms such as distributed ledger technologies to create audit and accountability mechanisms that are capable of detecting and avoiding counterfeit and fraudulent transactions.

---

<sup>10</sup> image distributed under Creative Commons CC0 courtesy of <https://www.pxfuel.com/en/free-photo-osvpk>

The goal of this demonstration case is to provide a blueprint for supply chain solutions across multiple sectors. One specific application in the energy sector involves protecting the supply chain for the production of transformers for power distribution, which are crucial components in power networks.

### 2.2.3 Privacy-preserving identity management

To identify ourselves in our everyday lives there are usually a small number of identity cards that we use: National ID, passport, driving licence, gym card, etc. When we want to provide some form of identification, we usually use our national ID or passport. Unfortunately, this kind of ID may include a lot of information that is provided unnecessarily. For example, suppose that a local restaurant provides free desserts to people on their birthday. In order to prove that it is really their birthday and get the free dessert, people may provide their ID. Unfortunately, their ID provides more information than is necessary, including name, surname, address, etc. It would be good to have a system that could manage several aspects of digital IDs and provide only the information needed, without the rest of the information that may happen to reside in the same ID. Such identity management systems could have a wide variety of applications, including eHealth, eGovernment, etc.

### 2.2.4 Incident Reporting

The Digital Single Market landscape and its transformation into a highly interconnected environment have led regulators to identify critical sectors and the need to draw attention to their systemic relevance. An analysis of all the actors involved in the scenario of a large cyberattack demonstrates that cyber risks transcend not only national borders, but also sectorial boundaries, leading to potentially dramatic systemic risks. This underlines the importance of taking a holistic view, pushing for a collaborative approach to enhanced cyber resilience.

Bearing in mind the objective of increasing readiness and awareness in cybersecurity, the current EU legal framework already incorporates the need to comply with **Mandatory Incident Reporting** to different Supervisory Authorities, respecting the relevant impact assessment criteria and thresholds, timing, data set, and means of communication, as defined by each authority at both the EU and national levels. All these different criteria and patterns cause fragmentation in the overall incident reporting process and have to be handled alongside the critical path of managing the incident itself.

### 2.2.5 Maritime Transport

The maritime transport vertical is a representative example of a collaborative and complicated process that involves domestic and international transportation, communication and information technology, warehouse management, order and inventory control, handling of materials, and import/export facilitation – among others. Maritime transport services include various interactions and tasks among the disparate entities engaged (stakeholders and actors), each having their own goals and requirements. In particular, these services include a number of interactions and tasks that involve several physical and cyber operations, interconnections and assets. These include docking of the ship, stevedoring, loading, unloading, storage, transportation, inspection, etc., as well as pre-arrival notifications, customs clearance documentation management, declarations to the International Ship and Port Facility Security, etc.

## 2.2.6 Medical Data Exchange



Figure 2: Collecting and re-using medical data is expected to result in breakthroughs in medicine<sup>11</sup>

Over the past few years patients, doctors, nurses, hospitals, health authorities, pharmaceutical companies and medical research organizations have started to generate a tremendous amount of medical data (see Figure 2). As more and more health examinations move from the paper/film world to the digital domain, and as people employ several self-monitoring health devices, the volume of medical data keeps increasing. Although the growing availability of digital medical data increases its value, at the same time it also provides a much wider target for cyberattacks.

This demonstration case integrates and validates the research outcomes regarding the cybersecurity and protection of sensitive medical and other personal data during data sharing in a realistic environment, through the DAWEX data marketplace platform. The results are intended to enhance multi-lateral trust among stakeholders, generating and consuming data in the medical business sector, preserving user data privacy, improving its trustworthiness and creating new business opportunities.

It will allow the secure and trustworthy exchange of sensitive data between the various stakeholders, including companies, public organizations and patients, each with different aims and claims, with regard to security, data protection and trust issues. These must be aligned with the applicable legislation and strategic policy framework, which includes the GDPR<sup>12</sup> (General Data Protection Regulation), NIS<sup>13</sup> Directive<sup>14</sup>, the blueprint for rapid emergency response, ENISA recommendations on security and privacy, etc.

## 2.2.7 Smart Cities

Over the past few years, automation in our everyday environments has noticeably increased. Smart devices that are capable of regulating everything from the water in large-scale facilities to the temperature in our

---

<sup>11</sup> image distributed under CC0 courtesy of <https://www.pxfuel.com/en/free-photo-ebbfr>

<sup>12</sup> <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

<sup>13</sup> NIS stands for Network and Information Security

<sup>14</sup> <https://eur-lex.europa.eu/eli/dir/2016/1148/oj>

homes have started to proliferate and will continue to do so in the future. As the associated sensors and actuators monitor and control significant parts of our everyday lives, they are bound to be considered by cyber attackers as potential targets. To address this challenge, smart cities are being forced to implement the appropriate mechanisms to provide their citizens with a safe and secure environment, assuring them of privacy and data protection by design and full control of how their personal data is processed.

To this end, it is important to identify measures, approaches and technical solutions that support responsible smart cities and stakeholders in the entire process of privacy and data protection, from risk assessment to solution elicitation and enforcement.

Smart city attacks can happen at least at two levels:

- The individual level (such as citizens and civil servants); and
- the organizational level (such as public authorities and third parties).

The two levels will need different kinds of tools and mechanisms:

- For individuals, tools related to social engineering, phishing, data ownership and possibly training.
- for organizations, tools related to risk assessment, predictive analysis, and mitigation activities, according to the existing legislation on data protection and privacy.

## 3 Open Banking

### 3.1 The Big Picture

Open banking is a banking practice that provides third-party financial service providers open access to consumer banking, transaction and other financial data from banks and non-bank financial institutions through the use of application programming interfaces (APIs). Open banking allows the networking of accounts and data across institutions for use by consumers, financial institutions, and third-party service providers<sup>15</sup>.

In a nutshell, open banking:

- Is a system for allowing access and control of consumer banking and financial accounts through third-party applications.
- Has the potential to reshape the competitive landscape and consumer experience of the banking industry.
- Raises the potential for both promising gains and grave risks to consumers as more of their data is shared more widely.

While the concepts around open banking had been in circulation for some time in several financial jurisdictions, regulators were also seeking to drive increased competition and innovation by opening up customer banking data to third parties. In Europe this was primarily through the Payment Services Directive, first adopted in 2007<sup>16</sup>.

In October 2015, the European Parliament adopted a revised Payment Services Directive, known as PSD2<sup>17</sup>, which updated and enhanced the EU rules put in place by the former legislation. These new rules included aims to promote the development and use of innovative online and mobile payments through open banking

The revised Payment Services Directive entered into force on 12 January 2016 and Member States were given until 13 January 2018 to transpose it into national law.

The aim of PSD2 was to modernise Europe's payment services to the benefit of both consumers and businesses; to enable innovative services, new market players, greater transparency and consumer choice, for promoting a digital single market within the EU and EEA and at the same time guaranteeing a high level of security.

<sup>15</sup> <https://www.investopedia.com/terms/o/open-banking.asp>

<sup>16</sup> Directive 2007/64/EC <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32007L0064>

<sup>17</sup> **Payment Services Directive 2**: Directive (EU) 2015/2366 (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366>) of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market amending Directives 2002/65/EC (<https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32002L0065>), 2009/110/EC (<https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32009L0110>) and 2013/36/EC (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013L0036>) and Regulation (EU) No 1093/2010 (<https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32010R1093>) repealing Directive 97/5/EC (<https://eur-lex.europa.eu/eli/dir/1997/5/oj>)

One of the best innovations comes from having third party providers in the payment chain being able to access bank accounts and make payments on behalf of customers, thus enabling the concept of open banking. To securely communicate, third parties and ASPSPs<sup>18</sup> can rely on dedicated interfaces (APIs), that should be properly configured to reduce the risk of frauds and attacks and are considerably better than screen-scraping which was the custom previously.

PSD2 enables bank customers, both consumers and businesses, to use third-party providers to manage their finances. In other words, as long as the user consents, companies other than a user’s bank are able to do things previously reserved for banks. This means that users may use a non-banking service to pay bills, make transfers to friends and analyse spending, while still keeping their money safe stored in their current bank account. Banks, however, are obliged to provide these third-party providers access to their customers’ accounts through open APIs, enabling these third parties to build services on top of the banks’ data and infrastructure. Hence, the banks are no longer only competing against other banks, but against everyone licensed to offer financial services. PSD2 fundamentally changes the payments value chain, the use of account information, what business models are profitable, and customer expectations. The directive introduces two new types of players to the financial landscape: the AISP (see Figure 3) and the PISP<sup>19</sup> (see Figure 4).

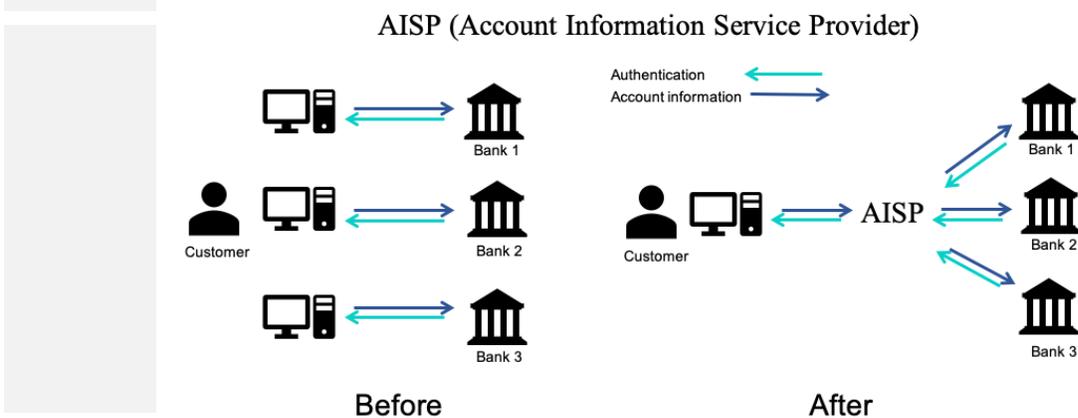


Figure 3: A simple personal finance management model

<sup>18</sup> ASPSPs: Account Servicing Payment Service Providers provide and maintain (current, savings and card) accounts, traditionally the core business of a bank.

<sup>19</sup> AISP: Account Information Service Provider - Any (registered) provider that wishes to aggregate online account information of one or more accounts held at one or multiple ASPSPs (banks). This service can be used in accounting or generation of dashboards for a single customer.

PISP: Payment Initiation Service Provider – Any licensed organisation (like a FinTech) that can initiate credit transfers on behalf of a client.

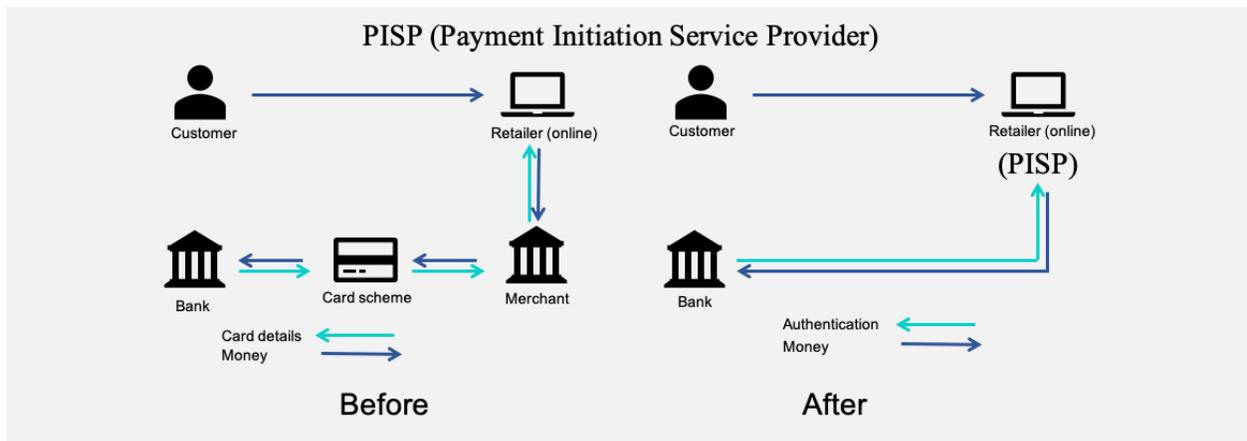


Figure 4: Payment Initiation Service Provider (PISP)

### 3.1.1 RTS SCA

The Regulatory Technical Standards (RTS)<sup>20</sup> on strong customer authentication (SCA) under PSD2 came into force on 14 September 2019, although it will only actually be fully implemented in 2022. They require PSPs<sup>21</sup> to adopt measures guaranteeing adequate levels of security to access and authorise remote payments, to properly operate with third parties and overall to increase the level of security of electronic payments to ensure consumer protection against fraud. Nonetheless, despite the security improvements, there remain some ‘gaps’ for fraudsters to exploit.

### 3.1.2 PSD2 and GDPR

Both the GDPR<sup>22</sup> and PSD2 share the same objectives – to put customers in control of their own data and to keep that data safe. However, because they were designed independently of each other without the regulators properly joining up the dots, there are deployment incongruities that could lead to security holes and vulnerabilities.

PSD2 provides that PSPs are entitled to access, process and store personal data necessary for providing their services if the payment service user (PSU) has granted explicit consent for this. However, apart from consent the GDPR enables PSPs to choose another legal basis for accessing, processing and storing personal data, such as the performance of a contract, legitimate interest or compliance with legal obligations based on national or EU law. Given this difference, it is debatable whether PSPs should limit themselves only to obtaining the PSU’s consent according to PSD2, or whether they could also use the other legal basis provided by the GDPR. According to guidance provided by the European Data Protection Board (EDPB), PSPs must comply with both PSD2 and the GDPR. This means that PSPs could also use the legal basis

<sup>20</sup> Regulation (EU) 2018/389

<sup>21</sup> PSP stands for Payment Services Provider

<sup>22</sup> Regulation (EU) 2016/679

provided by the GDPR as PSD2 is not a special legislation<sup>23</sup>, although there is no getting around the fact that both the GDPR and PSD2 have to be adhered to.

Under PSD2, third parties will be able to access customer account information directly, provided they have the customer's explicit consent, and enable the customer to exercise their right to data portability under the GDPR.

PSD2 also provides that a PSU's consent must be explicit. Instead, the GDPR requires explicit consent only in case of processing special categories of personal data. Both have special categories, and consent is carried out in different ways. As financial, payment and transaction data are not considered special categories of data, under GDPR, consent would be sufficient. The EDPB clarified that 'explicit consent' under PSD2 is an additional contractual requirement, different than the 'consent' under the GDPR, in the context of a contractual relationship, the legal basis for data processing would be 'performance of a contract' instead of the PSU's 'consent'. This means that PSPs must build an explicit consent mechanism in line with PSD2, whilst from a GDPR perspective they must rely on a different lawful basis (i.e. contractual necessity) to process personal data<sup>24</sup>.

In the payment process, there are also 'silent parties' who do not have a direct contractual relationship with the PSP, such as persons who have a bank payment account to which the PSU transfers money through the PSP.

As such, PSPs cannot ask 'silent parties' for contractual consent. The problem is that banks transfer their data (e.g. bank account numbers, name, address) to PSPs (especially to AISP and PISP) based on the legal provisions on strong customer authentication. From a GDPR point of view, AISP/PISP will process the data of the 'silent parties' based on their and the PSUs' legitimate interest<sup>25</sup>.

The GDPR also stipulates the responsibility of the data controller – in this case the bank or ASPSP – to safeguard their customers' data with the threat of considerable fines if there is a failure to do so. In this confluence of the objectives of both regulations, it's not clear which party is responsible for obtaining the customer's consent and, significantly, which organisation – the PISP or the ASPSP – is culpable if the customer suffers any loss due to a data breach or cyber-attack.

PSD2 states that PISP must not use, access or store any data for purposes other than the provision of the payment initiation service explicitly requested by the payer. Consequently, a PISP is not entitled to use the data collected other than for providing payment initiation services, even if the PISP had the PSU's consent under the GDPR.

The PSD2 contains a similar provision for AISP, but with an additional condition: "in accordance with data protection rules". It is unclear whether this additional obligation imposed on AISP has any relevance from a legal perspective. The competent EU authorities have yet to issue guidance on this. Although both the Romanian and Hungarian implementation laws have kept this wording from the directive, only the Hungarian Central Bank has adopted a position on this issue, considering that an AISP cannot re-use the

---

<sup>23</sup> [The interplay between PSD2 and GDPR](#), CMS Law-Now, April 2020

<sup>24</sup> *ibid*

<sup>25</sup> *ibid*

data collected to provide other services to the PSU, even with the PSU's consent under the GDPR. This interpretation creates a distortion of competition because, unlike AISPs, other market players (e.g. mortgage comparators), regulated or unregulated, enjoy a more advantageous legal position as they are allowed to use the same data to provide other services to the PSU<sup>26</sup>.

The link between PSD2 and GDPR is not just about monetary transactions but also the management of personal data. The discernible weaknesses are in ensuring that a third-party respect the GDPR and is adequately compliant as well as ascertaining where liability lies if there is any data breach.

### 3.1.3 European Data Strategy

On 19 February 2020, the EU published 'A European strategy for data'<sup>27</sup>, which observes the progress made by the EU in becoming '*a leading role model for a society empowered by data to make better decisions – in business and the public sector*'. This was followed on 25 November 2020 by a proposal for a Data Governance Act which stipulates, in essence, that data should move freely – its main impact will be to open up all industries to data sharing, not just banks. It references the steps made since 2014 in terms of the GDPR establishing a framework for digital trust, the Cybersecurity Act<sup>28</sup> and the Open Data Directive<sup>29</sup>: PSD2 provides the legislation on data access for payment service providers. The EC's conviction is that businesses and the public sector can be empowered through the use of data to make better decisions with the aim of creating a single European data space where personal as well as non-personal data, including sensitive business data, are secure allowing business access to '*an almost infinite amount*' of high-quality industrial data. Core to this vision is the empowerment of individuals to exercise their rights through legislation and appropriate enforcement mechanisms, as is evidenced by the initiatives of MyData Global<sup>30</sup> and others to give individuals the tools and means to decide at a granular level what is done with their data. This architecture would imply the emergence of a new type of actor, the data operator, who could contribute to a new form of fragmentation of the supply chain of open banking and/or digital services, thus potentially introducing new vulnerabilities and making the current open banking security roadmap even more relevant.

The EC recognises that there are plenty of challenges and obstacles that have to be addressed or overcome in pursuit of this strategy, but the groundwork is being laid and it will have consequences for the way in which banks and other financial institutions approach the management of data. The EC intends to promote the development of common European data spaces in '*strategic economic sectors and domains of public interest*'. The role of the envisioned Common European financial data space is to '*stimulate, through enhanced data sharing, innovation, market transparency, sustainable finance, as well as access to finance for European businesses and a more integrated market*'. To achieve these objectives, a keen observance of new and existing cybersecurity risks and vulnerabilities will be of the highest importance.

---

<sup>26</sup> *ibid*

<sup>27</sup> Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM (2020) 66 final, Brussels, 19 February 2020

<sup>28</sup> Regulation (EU) 2019/881

<sup>29</sup> Directive (EU) 2019/1024

<sup>30</sup> <https://mydata.org>

### 3.1.4 Summary

As identified above, there are unresolved issues<sup>31</sup>, both today and in the future, which are inhibiting the full realisation of the objectives of PSD2 and Open Banking, which have key roles to play in the drive towards the European digital single market and a data-agile economy.

PSD2 was intentionally drawn up not to be prescriptive in how it should be applied by financial institutions or in Member State legislations, in order to facilitate a greater degree of innovation. However, this presents a series of challenges that are addressed in this roadmap:

Given the fragmentary disconnected nature of the Open Banking landscape across Europe and beyond, there are no:

- clear rules associated with end-to-end processing (Challenge 1)
- established mechanisms to monitor the lifecycle of stakeholder relationships (Challenge 2)
- guarantees of seamless cross-border interoperability (Challenge 3)

Authentication plays a key role in making Open Banking work and there are two dimensions to this:

- Among the assumed benefits of PSD2 and Open Banking is that it will provide gains as well as grave risks to end users: the gains come with the transparency and consumer choice, but only if authentication is convenient and compliant (Challenge 5), and one of the risks results from not having adequate means to ensure critical real-time decision-making with regard to access (Challenge 4).
- One overlooked area in Open Banking is its impact on B2B transactions, where not enough consideration is given to how real-world authentication processes can be translated to the corporate world (Challenge 6).

## 3.2 Overview

We are seeing the increased usage of the open data economy. Previously, large corporates and whole industries, such as telecommunications, used to be based on closed systems, private protocols, hidden interfaces and proprietary architectures. Today almost all industries are increasingly adopting open systems, standard interfaces and protocols. This has partially been driven by the own regulation (to open up monopolies) and by the realization of the affected stakeholders themselves that open systems can lead to massive benefits. Every industry has realized the benefits of open data: transportation has been revolutionized by companies like Uber, accommodation has been transformed by companies like Airbnb, and others, all of whom have been able to do this because of the prevalence of open services. In the case of Uber, for example, the company's novel proposition has been successful through combining the locations of the passenger and driver (both available via open standard APIs from their mobiles) and the open standard GoogleMaps and PayPal APIs. This mashup economy, where open data and interfaces are connected in creative ways, is changing the way all industries operate.

---

<sup>31</sup> See section 3.3

It has led to a tremendous growth in the impacted markets – people travel and communicate much more – to the benefit of the associated industries. This in turn has led to massive new competition – benefitting new start-ups – and offering much more choice, more transparency, lower costs, and better service to users.

The financial services industry has so far largely resisted this trend. Often citing real or imagined security reasons – and some may say to keep competitors at bay – the data and financial services have remained largely closed. However, increasing pressure from regulators, consumers and concern about new attackers, such as FinTechs, accessing bank data anyway via screen scraping, has recently forced this industry to open up as well: especially since it has become clear that open systems can be made secure, although there are challenges.

A worldwide leading development of this Open Banking is to be found in Europe’s PSD2 which is forcing all 4,000 banks in 27 Member States<sup>32</sup> to provide open access to standard services (initiating a payment) and data (transaction history) via APIs on customers’ bank accounts. Not surprisingly, this is turning the concepts of mobile and e-commerce and wider financial services on their heads.

The finer details of the directive and how exactly PSD2 is enabling this open access and what measures are being put in place for third party access to users’ bank accounts, their payments and their transaction data will not be discussed here. Suffice it to say that opening up whilst still ensuring data protection, user consent and cybersecurity is clearly a major challenge. It is of course of ultimate importance to guarantee the protection of Europe’s consumers’ and companies’ money and data.

This section aims to show some of the new use cases that are emerging due to PSD2 and Open Banking to enable mobile and e-commerce and what some of the key security challenges are that need to be solved. Only then will we reap the benefits in financial services and mobile and e-commerce in a safe and secure way as seen in other industries such as transport, accommodation, telecommunication, and others.

### **3.3 What is at stake?**

At stake are not only the financial assets of banks and their customers, but also customer data and the brand recognition of the numerous actors in the financial ecosystem. It is clear that the topics of access by third parties to users’ data and the ability of third parties to initiate payment from a users’ bank account are highly sensitive. Never must an access be allowed to any party that is not licensed, nor must access be allowed to any data that has not been explicitly consented to by the user. Unfortunately, as the above section has shown, a large number of actors must work together: users, client software providers, FinTechs, service providers, banks, national and European regulatory bodies. The key is thus to secure an unbroken and unbreakable chain of trust all the way through this complex eco-system.

Many topics on security and privacy have been described in great technical detail by the primary and secondary regulation. Strong customer authentication, the elements that must be employed here, the

---

<sup>32</sup> Although the UK formally left the EU on 31 January 2020, the former Member State remains in ‘transition’ until 31 December 2020, with no certainty on its future position on PSD2. See also section 3.5.7.

exemptions, are described over many chapters by PSD2 itself – and several EBA RTS<sup>33</sup>, guidelines and FAQs. Also, non-PSD2 regulations, notably GDPR<sup>34</sup>, are highly relevant and must of course be observed for any data access and use.

### 3.3.1 What needs to be protected?

The primary assets to be protected are the bank or financial institution’s customer data and financial assets as well as the reputational loss associated with its brand and standing with customers and business partners.

### 3.3.2 What could go wrong?

It’s not difficult to envisage a scenario where a bank simply does not trust a TPP<sup>35</sup> claiming to act on behalf of one of its own customers, resulting in either loss of service – if the customer has in fact entrusted the TPP – or loss of data and/or finances if the claim is not genuine. Essentially, banks are having to forego long established mechanisms for knowing who they are transacting with.

### 3.3.3 Social Engineering & Malware Attacks

New threat scenarios can arise due to the presence of third parties posing between users and ASPSPs, in terms of:

- attacks to data and information stored by and exchanged with a third party
- new social engineering attacks where the fraudsters contact the customer pretending to be the third party
- Based on an analysis of 1.9 billion digital transactions in the ThreatMetrix Q1 2018 Cybercrime Report: Europe Deep-Dive.<sup>36</sup> European digital businesses suffered 80 million fraud attempts, experiencing more pronounced spikes of peak attack periods throughout Q1 2018 compared to previous years. Identity spoofing has become a major threat across the region, resulting from stolen personal data now available on the dark web. In Germany, for example, identity spoofing attacks have more than doubled compared to Q1 2017, according to the official press release of the report. Moreover, 60 million ecommerce transactions were rejected as fraudulent in Q1, which is a 47% increase over 2017. There is a particular focus on identity testing activities targeting this sector, with fraudsters looking to capitalise on the low-friction approach taken by many merchants, aimed at increasing online revenues and encouraging customer loyalty in a fiercely competitive market.<sup>37</sup>

---

<sup>33</sup> European Banking Authority Regulatory Technical Standards – see [Regulatory Technical Standards on strong customer authentication and secure communication under PSD2](#)

<sup>34</sup> [General Data Protection Regulation](#): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

<sup>35</sup> In PSD2 a third-party provider (TPP) can be a Payment Initiation Service Provider (PISP) or an Account Information Service Provider (AISP). Banks, financial software providers, retailers, telcos, FinTechs, and big techs are all parties that can become a TPP.

<sup>36</sup> <https://www.businesswire.com/news/home/20180516005314/en/ThreatMetrix-Finds-Digital-Transactions-in-Europe-Bombarded-with-a-30-Increase-in-Cyberattacks-as-Mobile-Emerges-as-the-Secure-Channel>

<sup>37</sup> [https://www.thepayers.com/digital-identity-security-online-fraud/europe-hit-with-a-30-percent-increase-in-cyberattacks-threatmetrix-reports/773196-26?utm\\_campaign=20180517-automatic-newsletter&utm\\_medium=email&utm\\_source=newsletter&utm\\_content=](https://www.thepayers.com/digital-identity-security-online-fraud/europe-hit-with-a-30-percent-increase-in-cyberattacks-threatmetrix-reports/773196-26?utm_campaign=20180517-automatic-newsletter&utm_medium=email&utm_source=newsletter&utm_content=)

A major problem for all banks is how the use of mobile phones exposes a major vulnerability from not having two separate execution elements in a single device for accessing bank account information as specified in PSD2 RTS Article 9 “Independence of the Elements”<sup>38</sup>. Although the devices themselves demonstrate adequate security and are not themselves susceptible to attack, the increase in the volume of social engineering attacks exposes user bank accounts to attacks that cannot be easily recognised or intercepted by the banks – and represent a different dimension to technology-based issues. On the other hand, mobiles can also be seen to have a very positive impact through the availability of different forms of biometrics which help provide a single point of failure. VISA, for example, use phone sensors for authentication purposes.

Banks have become highly successful at intercepting malware attacks by recognising, through sophisticated tooling including machine learning and other forms of predictive analysis, anticipated user behaviours when accessing their accounts. However, with the introduction of PSD2, customer bank accounts will be accessed by third parties (PISPs) making it much harder for the banks’ systems to identify between genuine access requests and malware.

### 3.3.4 Certificate Verification

Even after the AISP (and the third party) registers with a national certificate authority (NCA), the ASPSP is not able to verify the certificate electronically, as currently the registration is not accessible online<sup>39</sup>. An EU-wide mandatory and standardised exchange between CAs on business model assessments under PSD2 is of specific importance for innovative services and models which was not considered when PSD2 was finalised.

When the PSU wishes to revoke the authority given to the PISP, they are faced with an exacerbation of the problem outlined immediately above, especially due to the necessity for real-time revocation.

### 3.3.5 GDPR & PSD2

Under PSD2, third parties will be able to access customer account information directly, provided they have the customer’s explicit consent, and enable the customer to exercise their right to data portability under the GDPR. The GDPR also stipulates the responsibility of the data controller – in this case the bank or ASPSP – to safeguard their customers’ data with the threat of considerable fines if there is a failure to do so. In this confluence of the objectives of both regulations, it’s not clear which party is responsible for obtaining the

---

<sup>38</sup> <https://eba.europa.eu/sites/default/documents/files/documents/10180/1761863/314bd4d5-ccad-47f8-bb11-84933e863944/Final%20draft%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2%20%28EBA-RTS-2017-02%29.pdf?retry=1> p.22

<sup>39</sup> Although NCAs provide the information about payment and electronic money institutions authorised or registered within the EU and the EEA to the EBA and are responsible for its accuracy and updating that information regularly, at least once per day, subject to changes in their national registers, in accordance with Article 11 of PSD2, granting of authorisation remains under the remit of the individual NCAs.

customer's consent and, significantly, which organisation – the PISP or the ASPSP – is culpable if the customer suffers any loss due to a data breach or cyber-attack.

The link between PSD2 and the GDPR is not just about the handling of money but also the management of personal data. The discernible weaknesses are in ensuring that a third party respects the GDPR and is adequately compliant as well as ascertaining where liability lies if there is any data breach.

In making a payment to a third party, unless the third party is trusted by the PSU, the PISP opens up a potential vulnerability in terms of financial loss but more importantly a lack of certainty in case of a data breach or data misuse.

PSD2<sup>40</sup> forbids banks sharing “sensitive payment data” with third parties, but there is no clear definition of what it is. Without clarification banks will err on the side of safety, particularly from the perspective of GDPR compliance.

### 3.3.6 APIs

The lack of a standard and universally applied API in Open Banking is a barrier to greater harmonisation in Europe and beyond. However, it may be questionable as to whether it also poses a security risk. On the one hand, it provides a single point to fix, and yet perhaps diversity, with a plethora of API standards, may improve security i.e. no single point of failure.

Consumer-authorized data access has grown very rapidly in recent years, bringing with it a wide variety of innovative new products developed by organisations unfamiliar with traditional banking and other financial institutions, often in haste to get to market as quickly as possible. This has led to mistakes being made through data exposure and leakage via the APIs, which by their very nature makes them dangerous. For example:

- **API security is not widely understood by banks**, because of a lack of API security expertise that impacts all parts of a product's lifecycle, from development to QA to security to compliance.
- **Developers mistakenly expose more data than they should**, often in an effort to improve the customer experience, making it easier for bad actors to abuse the API or business logic.<sup>41</sup>
- **Private APIs published out of sight by the security team** are probably rarer in FinTech than in other industries, yet they pose a significant risk and must be reined in. Developers and security must work collaboratively to publish secure APIs and manage the entire lifecycle. Similarly, deprecated APIs not fully removed from public availability have to be managed effectively.
- **APIs make the PSD2 exfiltration of data easy and fast**, allowing for massive amounts of data to be moved with little effort: a great feature for bad actors and a bad headache for security and compliance teams.

---

<sup>40</sup> Article 66: Rules on access to payment account in the case of payment initiation services; Article 67: Rules on access to and use of payment account information in the case of account information services

<sup>41</sup> For example, hidden parameters can lead to threats like privilege escalation, and confidential or sensitive data could also be exposed in verbose error messages or response codes which is one of the Open Banking Architecture use cases – see [Deliverable D5.2: Specification and Set-up Demonstration case Phase 1](#)

Passing information over Open Banking has undoubted benefits, but it has introduced a commercial phenomenon of attack tools and bots. This means that all aspects of the production, maintenance and consumption lifecycle of Open Banking APIs must pay keen attention to the security risks.

New threat scenarios can arise due to the presence of third parties posing between users and ASPSPs, in terms of attacks to the availability of APIs and other interfaces services

For PISPs and ASPSPs not utilising the same ‘open banking API’, some form of mediation may be used that may introduce an unforeseen security risk.

Some FinTechs may want to continue to use screen-scraping as well as web-scraping including APIs, attempting to simulate a bank’s interfaces. Some banks may continue to offer it since they are not API-ready and/or because the national authority does not find their API solution sufficient and they thus have to offer “direct access” a deep type of access that avoids verification.

In these cases, PSD2/RTS/GDPR demand that the third party be reliably identified and only access data that is allowed.

How can that be ensured in a screen-scraping environment? If a third party impersonates a user logging on to online banking, identification (i.e. it really is that rogue third party) and restriction of access (i.e. not looking at all the other data seen on the browser screen) are very difficult and a real security/GDPR challenge.

### 3.3.7 Bank Administration

A different set of security challenges is presented in the scenarios described above when the user is a corporate administrator. Although most PSD2 focus is on consumers, some of the often-neglected areas of the regulation but with high potential are the new opportunities for corporates. The special requirements of corporates<sup>42</sup> present an additional layer of complexity and security risks in the context of PSD2.

Another issue is how to secure a bank’s information systems. Specifically, how to verify that the security policies of TPPs’ that interact with the bank are compatible with those of the bank. More generally, how can a bank trust how TPPs’ security mechanisms work, an issue which is not just relevant to PSD2?

The issue is not just with users but between partners, requiring that security mechanisms should be flexible. Today’s bank perimeter is moving, with TPPs coming and going. Security comes to the weakest link requiring an evaluation and maturity assessment of each partner.

### 3.3.8 Circles of Trust

PSD2 should not be seen as a constraint but an opportunity, presenting options to develop new types of services, such as building an eco-system of partnerships. However, there is an issue with how to securely authenticate each partner and to create a ‘circle of trust’: if not carried out effectively, there will be a security vulnerability.

---

<sup>42</sup> For example, multiple roles of authorising users, multiple signatories, authentication depending upon limits, etc

### 3.3.9 What is the worst thing that can happen?

The worst thing that can happen to a bank or financial institution is that it gets so badly attacked that both the institution, its customers and other stakeholders in Open Banking are severely impacted. The examples given below apply not only to Open Banking scenarios but electronic banking in general.

- For the **institution** this could mean,
  - If an attacker is able to successfully carry out an attack that allows them to fraudulently siphon off the financial assets of multiple high value customers, the institution would have to make such substantial and potentially crippling compensatory payments to those customers that it would no longer be financially viable and have to go out of business
  - If a major system attack resulting in the loss of money or data or both turns out to have been the result of significant negligence on the part of the institution, and if the institution is not able to contain the resulting media exposure, it would have such an impact on the brand and reputation of the institution that it might not be able to recover.
  - It is a well-documented phenomenon, that, after one successful attack, an attacker who remains undetected goes on to carry out further attacks at other institutions over the following weeks and months<sup>43</sup>. If it turns out that the institution that suffered the initial attack had not made sufficient effort to notify institutions in the second wave of attacks, there could be unpleasant recriminations, particularly if all the institutions were part of the same corporate structure.
- For the **customer**:
  - If a customer incurs a pecuniary loss as a result of an attack, the bank has a responsibility to make good the loss; so, the consequences would be inconvenience and a loss of trust in the institution, which could result in the customer seeking another institution
  - If the institution has suffered an attack resulting in a data breach, the consequences could extend well beyond the customer's relationship with the financial institution. In addition, in the case of data loss in the context of Open Banking, it remains unclear as to where liability for compensation lies. For example, if a malevolent merchant accesses the bank through a TTP and gets access to customer data that subsequently is misused in one of many different ways resulting in a financial claim by the customer, both the institution and the TTP could deny responsibility and hence liability.
  - Nevertheless, after a financial loss, the procedures for customer compensation are relatively straightforward – the customer will get compensated. However, after a data loss with its reputational implications for a customer's brand, it's not clear where the liability lies or how a fair level of compensation could be assessed.
- For the **regulator**:

---

<sup>43</sup> This is the rationale for the OBSIDIAN use case and demonstrator as described in [Deliverable D5.1: Requirements Analysis of Demonstration Cases](#) and [Deliverable D5.2: Specification and Set-up Demonstration case Phase 1](#)

- Although PSD2 and the various resultant open banking initiatives have received considerable enthusiasm from FinTechs and most banks, the general public does not fully understand how it operates and there is even now a certain wariness about the concept of banking being open: it appears counterintuitive and most people tend to be conservative when it comes to how their finances are managed. Hence, in the case of a highly visible attack as a consequence of Open Banking, both financial institutions and the public will lose confidence in trusting open access to their accounts. In some cases, this may suit the banks but could badly affect FinTechs.
- For the **Digital Single Market**:
  - Each and every publicised cybersecurity incident, particularly those impacting formerly well trusted financial institutions creates uncertainty and potentially panic that undermines and erodes trust in the digital world. Trust once lost is difficult to restore. For the digital economy this is a real setback.

### 3.4 Who are the attackers?

The threat agents could be any one of cyber-terrorists, hackers, economic adversaries, insiders, etc. Each one could have their own reason for an attack – from ransomware, direct financial gain to competitive advantage.

- **Hackers** are individuals or groups of individuals who employ an opportunistic mind-set, often falsely presenting themselves as bona fide customers using false or falsified documentation and usually act under simple profit motives.
  - **Data miners** or professional data gatherers who acquire information through cyber methods without sometimes infiltrating an organisation.
  - **Disgruntled or desperate customers**, who are driven to take advantage of access to a bank or finance company for financial gain
  - **Individuals, including ‘script kiddies’**, with absurd purposes prepared to cause mischief simply for the sake of it
- **Insiders** include:
  - **Professional data gatherers** posing as trusted insiders, generally with a simple profit motive;
  - **Non-ethical individuals** who are prepared to take advantage of their position within the bank in order to make profit for themselves or act on behalf of external criminals.
  - **Disgruntled employees**, who could be current or former employees seeking to damage the bank or finance company they have or have had a working relationship with
  - **State-sponsored spies** who have been planted inside an organization in order to support the idealistic goals that go along with this kind of occupation.
  - **Business partners** who go after inside information in order to gain financial advantage over competitors
- **Adversaries** comprise:
  - **Economic adversaries** are generally competitors in contesting businesses that compete for revenues, resources and clientele.

- **Legal adversaries** or ill-willed individuals who take part in legal proceedings against the company, warranted or not.
- **Cyber terrorists** in the context of Open Banking could include foreign states, wishing to destabilise the financial infrastructure of a targeted nation but more broadly speaking this group of attackers could also include
  - **Anarchists** are individuals who reject all forms of structure, either private or public, and act within few, if any constraints.
  - **Civil activists** are peaceful but highly driven individuals actively supporting a cause.
  - **Cyber vandals** are individuals who take amusement from penetrating and damaging existing assets and usually don't have a specific agenda.
- **Radical activists** are individuals who are highly motivated to support a cause and are open to destructive or disruptive methods.

### 3.5 Major incidents in this vertical

There have been surprisingly few major incidents that can be directly attributed to Open Banking: the world is waiting anxiously for Open Banking fraud to kick off, but so far not much has happened. This may be because there are such rich pickings elsewhere and Open Banking is still relatively new. For example, fraudsters are finding such profitable avenues in cards and in APP fraud (faster payments etc.).

However, when Open Banking transactions scale to large volumes, the fraudsters will surely strike.

#### 3.5.1 Phishing

One major fraud related to Open Banking took place in early October 2021, when millions of (British) pounds were stolen from Barclays accounts in a phishing scam by a fraudster using a Monzo account and a PISP.<sup>44</sup> A similar incident took place in May 2021, when the victim clicked on a text message link to verify a payment and was taken to a phishing website that mirrored the victim's bank. The cyber thief then swiped the victim's login credentials, set up an account and used the PISP to initiate payment requests. That incident prompted the OBIE<sup>45</sup> steering group to discuss the possibility that open banking payments were more exploitable because of the varying methods used for fraud prevention and detection along the payment journey.

#### 3.5.2 Decentralised Finance

According to a recent report,<sup>46</sup> just over 12 billion USD in losses have been suffered over the past year by Decentralised Finance (DeFi) users and investors. Again, this is only tangentially related to Open Banking. DeFi defines a flourishing alternative financial system that replaces traditional intermediaries with software running on blockchains. The prevalence of DeFi theft and crime is largely due to the untested and immature nature of the technology available. Mistakes in the design and development of decentralised apps are the most common cause, giving rise to bugs that hackers can exploit, accounting for 10.8 billion USD of all losses. Another 1 billion USD in losses are the result of exit scams (where a decentralised app creator

<sup>44</sup> <https://www.pymnts.com/news/security-and-risk/2021/barclays-hit-in-phishing-scam-using-monzo-account-pisp/>

<sup>45</sup> OBIE: [Open Banking Implementation Entity](#). See also 3.6.14 Challenge 3: Cross-border cooperation under differing legislation and security controls

<sup>46</sup> <https://www.finextra.com/newsarticle/39243/defi-fraud-and-theft-losses-reach-105-billion-in-2021>

intentionally leaves a “backdoor” in the code that allows them to steal users’ funds) and the theft of admin keys. One of the authors of the report acknowledged that,

*“Decentralised apps are designed to be trustless in that they eliminate any third-party control of users’ funds. But you must still trust that the creators of the protocol have not made a coding or design mistake that could lead to a loss of funds.”*

A Bank of England deputy governor observed that the highly decentralised and global structure of the DeFi sector, along with the difficulty in tracing end users, provides a unique set of challenges for regulators. He added that, “The sector is opaque, complex and undertakes financial activities that carry risk – activities that are regulated with the traditional financial sector. There are pronounced market integrity challenges given the absence of investor protection, AML and other market integrity provisions.”

Although not directly related to Open Banking as such, this loss report and associated risk warnings are salutary, given the hype that has surrounded the opportunities for the introduction of new technological trends in financial systems in recent years, particularly with respect to blockchain and other distributed ledger technologies, in the context of both traditional and challenger banks.

### 3.5.3 Authorised Push Payment (APP)

APP scams happen when a person or business is tricked into sending money to a fraudster posing as a genuine payee. Banking systems have automated security checks on suspicious activity, making it more difficult for criminals to steal money. As a result, they are targeting human weaknesses through APP scams using phone calls, emails, text messages, fake websites and social media posts to trick people into handing over their personal data, before conning them into authorising payments to them.

These types of scams can have a devastating impact on the people who fall victim to them. In 2020 APP scams were the second largest type of payment fraud, following card fraud, in both the volume of scams and the value of losses. However, the situation has since changed.

According to UK Finance, a banking trade body, there were 66,247 cases of APP fraud reported in the first half of 2020, with losses of 207.8 million GBP. There are eight types of APP scams, which are either:

- **malicious payee:** for example, tricking someone into purchasing goods that don’t exist or are never received.
- **malicious redirection:** for example, a fraudster impersonating bank staff to get someone to transfer funds out of their bank account and into that of a fraudster.
- In August 2019, the Payment Systems Regulator (PSR) gave members of the UK’s six (now nine) largest banking groups<sup>47</sup> a specific directive to implement confirmation of payee (CoP) by the end

---

<sup>47</sup> Barclays Bank UK plc The Co-operative Bank plc, HSBC UK Bank plc, Lloyds Banking Group, Metro Bank plc, Nationwide Building Society, National Westminster Bank plc, Santander UK plc and Starling Bank

of March 2020. The PSPs subject to the directive were involved in around 90% of FPS and CHAPS transactions. The directive was modified in February 2020 to allow an additional basis under which a directed PSP could apply for an exemption from an obligation under the directive.

In July 2020, the PSR confirmed that the directed PSPs had achieved widespread implementation of CoP, with certain agreed exemptions. This marked a significant milestone in addressing APP scams, but there is a strong desire to continue to expand the protection offered by CoP, so all PSPs, big and small, are being encouraged to implement CoP if and when the rules and standards apply to their accounts.

With confirmation of payee (CoP), banks can check the name on a new payee's account as well as the sort code and account number. Customers setting up a new payee (or changing details of an existing payee) will be able to confirm that the name they have entered matches the one on the account they intend to pay, helping to prevent payments going to the wrong account. Alerts notify the payer whether there has been a match, a close match or no match, meaning corrections can be made before the payment is sent. The service is designed to prevent misdirected payments as well as fraudulent ones.

The success of CoP depends on PSPs working together to prevent businesses and consumers from being defrauded. With that in mind, Pay.UK, the operator of the UK's payment systems, designed rules and standards for PSPs to follow when launching the service.

In addition, in 2019 the regulator instituted a contingent reimbursement model (CRM) code aimed to reduce both the occurrence and impact of APP scams, and designed to give people the confidence that, if they fall victim to an APP scam and have acted appropriately, they will be reimbursed. The arrangement was updated in 2020 and again in April 2021.

Nevertheless, despite these measures, currently more money is being stolen through APP scams than through card fraud, as criminals have found ways to avoid the automated checks within banking IT systems. According to UK Finance, there was a 71% increase in APP fraud in the first six months of 2021, reaching 355 million GBP. During the same period, payment card fraud dropped by 9% to 262 million GBP.

Overall, the amount of money lost to fraudsters in the UK reached 754 million GBP, a rise of 30% from the equivalent period last year, which UK Finance described as being at a level where it poses a national security threat and is calling for government-coordinated action across all sectors to tackle the issue.

Total unauthorised fraud losses, including card fraud, were 398.6 million GBP, a 7% increase on 2020. Looking at the positives, the banking and finance industry successfully blocked 736 million GBP worth of attempted frauds – 6.49 GBP in every 10 GBP of attempted fraud

## **3.6 Research Challenges**

The challenges identified below on security and privacy in an open system (which some see as an inherent contradiction) and how to protect data while opening up (which poses some challenges between PSD2 and GDPR), are both general, as well as concrete.

### **3.6.1 State of the Art**

#### **3.6.1.1 Summary**

Since 2019 not much has got better: there is still no end-to-end mapping, nothing on real-time revocation, nothing on delegated authentication, while Europe’s Open Banking is falling further behind. Some topics have even got worse, for example Brexit, regulatory divergence is not being addressed sufficiently, Europe continues to focus on the instruments of the last few decades (especially cards), some technologies highly disruptive to our current security, such as quantum computing<sup>48</sup>, are getting closer, and data breaches are exploding<sup>49</sup>.

However, there is increasing regulatory and market clarity on some key security topics, the focus on B2B in Open Banking continues to be strong, there is a massive drive towards “instant”, and—most importantly—there have not (yet) been any major reported cyber breaches based on Open Banking. Having said that, several specific fraud challenges have manifested, including account takeover and most notoriously Authorised Push Payment (APP) scams (see section 3.5.3). As banks and other financial institutions apply various fraud mitigation controls to prevent this digital fraud, there are signs that during the COVID-19 pandemic, fraudsters have systematically started to turn their attention to Open Banking<sup>50</sup>.

The regulator is putting increasing pressure on banks to create a continental harmonised payment scheme that will change the landscape. If banks do not step up, then the central bank will issue its own digital currency (CBDC), with enormous consequences for the balance sheets and structure of commercial banks. This new digital currency will not be based on blockchain, a topic whose hype has now largely gone away.

Furthermore, the regulator has published a whole series of documents that extend into wider multi-industry data sharing, opening up many opportunities—and new cyber risks, if they are not managed properly. The EU is putting more emphasis on eIdentity as the necessary bedrock of all digital services<sup>51</sup>, as is demonstrated by the update to the eIDAS regulation (‘eIDAS 2.0’), published in June 2021 which would give all EU citizens the right to carry an EU ID in a digital wallet for use in both the public and private sectors. COVID-19 has caused a massive push on digital services with many impacts on banking and finance and payments, as well as ways of working. These topics will be explored in more depth below, often with some concrete proposals where (new) security issues have arisen, and we will examine which of them may thus benefit from CyberSec4Europe investigation and use case demonstration.

### 3.6.1.2 The Bad News

---

<sup>48</sup> See ‘Disruptive technologies’ below

<sup>49</sup> <https://fortunly.com/statistics/data-breach-statistics/#gref>

ENISA Threat Landscape 2020 - Data Breach: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-data-breach>

<https://securityboulevard.com/2020/07/2020-is-on-track-to-hit-a-new-data-breach-record/#:~:text=We're%20just%20halfway%20through,a%20new%20data%20breach%20record.&text=According%20to%20researchers%2C%208.4%20billion,saw%20only%204.1%20billion%20exposed>

<sup>50</sup> <https://blogs.lexisnexis.com/fraud-and-identity-in-focus/uk-lockdown-sees-rise-in-open-banking-cyber-fraud/>

<sup>51</sup> <https://ec.europa.eu/digital-single-market/en/e-identification>

<https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/digital-identity-services/trends>

### **3.6.1.2.1 End-to-end view**

The industry would benefit from drawing up a true end–end landscape in Open Banking, from the consumer, through the value chain/customer journey across various service providers, the banks, the merchants/corporates and regulatory bodies. To date, as far as we know, no such map exists.

Since attacks typically go for the weakest link in the chain, it would be good to see the chain, where the weak links are, whether all the pieces are joined up, so that structural threats can be identified in advance and remedies sought. See also section 10.1.

### **3.6.1.2.2 Real-time revocation**

Much regulatory effort has been put in to allowing new entrants such as FinTechs to be controlled and licensed. In brief: a FinTech needs to prove to its home regulator that it is safe and adheres to the right processes, whereupon it will ultimately be granted an electronic certificate that it can then present to banks to gain access to customer accounts.

This works tolerably well. However, no provisions have been put in place to revoke such a certificate if a FinTech later defaults or changes its behaviour after granting of the licence.

Malicious actors must be removed from the ecosystem, in real time—not waiting for some fax to be processed in a government department before the weekend—and across all countries where the license has been passported.

Thus, there is a dire need for a real-time certificate management system, including not only issuance but also modification (e.g. withdrawing maybe only sub-rights) and complete instant withdrawal and shutdown.

### **3.6.1.2.3 Delegated authentication**

A core element of Open Banking is that access must only be granted after “informed customer consent”. Only then can a FinTech be allowed to read the customer’s transaction data and initiate a payment on their behalf. The regulated mechanism to verify consent is secure customer authentication, largely based on two of the following factors: knowledge, inherence, possession. The industry has finally got this extremely complex topic to work in a way that is both compliant and user-friendly (see under Good News below).

However, some topics remain open, for example in the key area of B2B different authentication methods are used from those in consumer methods, and these are often not supported yet. For example, if an SME wishes their tax advisor to access their corporate accounts, then the consent needs to be delegated from the SME to the tax advisor, who can then see the transactions to prepare the tax filings.

This, and a few other scenarios, are not yet catered for and would benefit from creative solutions.

### **3.6.1.2.4 Continental Europe**

Open Banking was “invented” in Europe. This was the first global geography to pass a law that all banks are mandated to open up with APIs to third parties and allow access—under control regimes—to customers’ transaction data and to initiate payments on their behalf.

This innovation leadership is currently being lost.

Internal wrangles between banks and FinTechs, rather than jointly trying to achieve a common good for the customer, are severely holding back progress. Finger pointing, technical fights over API standards and regulatory interpretations mean that PSD2, five years after publication, still has a long way to go.

By contrast, the UK picked up the topic enthusiastically, quickly set up a governing entity (OBIE) to drive the topic forward and to rapidly resolve any disputes between stakeholders and in the customer's interest; and furthermore is developing the system forward as needed. This means that the UK has a flourishing Open Banking ecosystem, with ever increasing traction<sup>52</sup>.

Half the European FinTechs are in the UK (the other half, partially passported, are in all continental Europe). FinTech unicorns are emerging almost exclusively in UK.

The UK model, and not the continental European model, is now spreading across the globe, being the role model for Japan, South America, Africa, ... up to Kazakhstan. As expected, the divergence between the UK and the European mainland continent has been exacerbated post Brexit (see section 3.6.9).

The good news is that Open Banking is conquering the world, and many see APIs and Open Systems as the end game, even though we are taking some detours (EPI, R2P<sup>53</sup> et al.) along the way.

Thus, it is worth putting major effort into this to identify all existing and coming security challenges for Europe, the UK and beyond. Solutions will be needed worldwide.

### 3.6.1.2.5 Cards vs Apps

There remains an unholy focus in Europe on cards (a system from 30 years ago), while the rest of the world is moving towards APIs, super apps and digital wallets<sup>54</sup>. The ECB is explicitly pushing cards, especially a pan-European card (since China, Russia, the US, etc. all have pan-continental cards while Europe does not).

However, the future is clearly not in cards, not even in virtual cards, but in services connected via APIs ("the API mashup economy") and in apps. As evidence for the latter, see the success of AliPay (now causing concerns even for the Chinese government, which feels a need to rein this in) and others in India (UPI), Indonesia (GoJek), etc. – see also section 3.6.9.2.

In Europe we do have some successful local app solutions (Blik, Swish, etc.), but nothing in the range or on the scale of the Chinese or US giants. For example, Alphabet has recently revealed their renewed proposal on Google Pay which looks very convincing to all. These data-hungry big technology companies will succeed as long as there is no privacy-conserving bank-based alternative.

Even the classical card incumbents (Visa, etc.) are seeing the writing on the wall. Mastercard is leading the charge, having even banished "card" from their logo, and now see themselves as a wider payment technology company, buying account-based companies (UK's ACH Vocalink), and massively investing in APIs (e.g. building hubs) and Open Banking (e.g. with fraud and directory services).

This trend is global, from South America to Asia, with the exception of Europe, which is still rooted in cards and is continuing to build new infrastructures on that basis. Smart FinTechs (such as Bluecode<sup>55</sup>) are

<sup>52</sup> <https://thefintechtimes.com/18bn-saving-open-banking/>

<https://www.cognizant.com/perspectives/open-banking-unleashed-or-is-it>

<sup>53</sup> Responsibility To Protect: <https://www.un.org/en/genocideprevention/about-responsibility-to-protect.shtml>

<sup>54</sup> See also section 3.5.8.2

<sup>55</sup> <https://www.trendingtopics.at/bluecode-ceo-christian-pirkner-in-europa-sind-wir-wirklich-an-allerletzterstelle/>

"Europe is in the last position"

exploiting the vacuum left in Europe for modern, API-based, FinTech-based, app-based, mobile-based services and are quietly building an international solution. Therefore, it is important not to follow the visible trend in the wrong direction, but to anticipate what will clearly be the future. Future solutions, as most people would agree, are based on the smartphone, not on cards.

### 3.6.1.2.6 Flagship projects

At the launch of Open Banking in Europe, while many were still wondering what this might be used for, Deutsche Bank and International Air Transport Association (IATA) received much press coverage for a joint project that would take \$8 billion in card fees out of the system using Open Banking. People can buy their air travel direct from their account, not via a card, and thus remove fees for airlines and customers.<sup>56</sup>

After the fanfares, this project—like a few other highly promoted flagships—is sadly no longer on the radar. This is not unusual in the highly dynamic world of payment innovations, where FinTechs become Unicorns overnight, others fail overnight, some technologies are massively hyped, others quietly succeed, while the market is changing with great dynamics.

Having said that, all is not lost. On 5 July 2021 one airline, Emirates, announced<sup>57</sup> the launch of Emirates Pay, a new account-based payment method for purchasing air tickets. Emirates Pay is now available for Emirates customers in Germany and the UK who are purchasing tickets via emirates.com. This makes Emirates the world's first airline to launch this payment alternative powered by a white-label solution jointly developed by IATA in partnership with Deutsche Bank.

There is a tendency, even in the professional media, to doom-monger about Open Banking rather than accentuating the positives. For Open Banking the significant takeaway is to look at the long-term trends (e.g. see B2B below), not just the individual spotlights.

### 3.6.1.2.7 Regulatory divergence

The difference in national regulations does not seem to be converging, at least not at the rate that is required. There is still a great deal of “regulatory arbitrage” leading international companies to choose the most favourable regulatory environment for themselves. Hence, we see hubs of online gambling companies in Gibraltar<sup>58</sup>, clusters of blockchain start-ups in Malta<sup>59</sup>, and many US giants setting up their European headquarters in Luxembourg (PayPal), Lithuania (Revolut) or Ireland (Google). The companies show where the regulatory control of data is weakest, the regulator most tolerant, the costs smallest, the processes most moved online, and where the most relevant regulations are interpreted in the most industry-friendly way.

---

<sup>56</sup> <https://www.openbankingexpo.com/news/deutsche-bank-pilots-disruptive-payments-solution-for-airlines/>  
<https://cib.db.com/news-and-events/news/db-pilots-payment-solution-with-iata.htm>

<sup>57</sup> <https://www.emirates.com/media-centre/emirates-first-to-launch-new-industry-payment-solution-in-partnership-with-deutsche-bank/>

<sup>58</sup> <https://www.theolivepress.es/spain-news/2017/01/05/how-gibraltar-became-one-of-the-worlds-biggest-gaming-hubs/>

<sup>59</sup> <https://www.recruitgibraltar.com/OnlineGamingCompaniesinGibraltar.asp>  
<https://www.quora.com/Is-Malta-the-best-place-to-establish-a-blockchain-startup>  
<https://www.meetup.com/topics/blockchain/mt/>

This shows that in the “single” market there is no level playing field and that there is large regulatory divergence.

To take a case in point, Google chose Ireland, since the data protection office there consists of only a handful of staff who are famously relaxed about data sharing. By contrast, companies in Germany, controlled by armies of data privacy regulators who are the strictest in the world, are at a major disadvantage to compete. To stay with this example, Germany even has some regulatory arbitrage within its own jurisdiction: each of its 16 Länder has its own Landesdatenschutzbeauftragte (privacy), Landesmedienanstalten (media), etc. This is a nightmare for a small Fintech that wants to focus on developing new customer-focused solutions rather than spending all its time just sorting out compliance.

This fragmented situation massively favours large companies that have large compliance offices to analyse this complexity and can set up their headquarters where it suits them best, giving them the biggest strategic advantage over competitors. Small start-ups will typically only be able to start in their home country and will have to live with whichever of the 16 NCAs (national competent authorities) they happen to have.

And then there will be the increasing regulatory divergence between continental Europe and the UK due to Brexit (see section 0).

If a way could be found to systematise regulatory applications (some dream of an XML schema describing how laws are implemented in each country, or each “Land”), then a country selection process and national compliance process could be much simplified.

#### **3.6.1.2.8 Disruptive technologies**

The massive impact of technologies on banking and payments has been apparent for some time. For example, from the early days of the Internet to:

- multimedia/multi-channel
- mobile and NFC – for contactless payments
- QR codes – see section 3.6.9.2 on Asian explosion of apps
- biometrics – face/finger recognition to improve user experience and security – no longer a choice of “either security or convenience”, one can now have both
- wearables – when your watch, your glasses and your ring are connected, you can make payments with a blink or a touch
- BLE – enabling beacons to pay automatically as you leave a shop, see Amazon Go - and general wireless device connection
- IoT – where your fridge will replenish food on your behalf
- “connected everything” – for example, cars paying for toll gates as they pass
- APIs – enabling “Open X” – the interconnection and mashup across all industries
- And more.

The massive impact of technologies on banking and payments has been apparent for some time. From the early days of the internet to multimedia/multi-channel, to mobile and NFC (contactless), QR codes (see section 3.6.9.2 on Asian explosion of apps), biometrics (face/finger recognition to improve user experience and security – no longer a choice of “either security or convenience”, one can now have both), wearables (where your watch, your glasses and your ring are connected and you can make payments with a blink or a

touch), BLE (enabling beacons to pay automatically as you leave a shop, see Amazon Go - and general wireless device connection), IoT (where your fridge will replenish food on your behalf), “connected everything” (e.g. cars paying for toll gates as they pass), APIs (enabling “Open X” – the interconnection and mashup across all industries) and more.

Currently, the use of AI on data is still at the beginning of a longer and larger journey (with many technical and ethical questions still unresolved); more mature is cloud computing (although the increasing dependence on US cloud services is causing some concern); and many further technological developments are in the making.

### 3.6.1.2.9 Quantum Computing

Looking a little further ahead, some extremely disruptive technologies are coming ever closer. A prominent example is quantum computing. This is not yet working reliably at scale – only a few, still very expensive, qubits can currently be managed at one time – but it is clear that this will become a major feature of the computing world of tomorrow.

Quantum computing does not rely solely on bits holding values of either 1 or 0, but on qubits that can be in several states (not only 0 and 1) simultaneously. This results in some properties not seen in the classical von Neumann architectures we have been relying on since the 1950s. The new quantum computers use physical quantum effects, such as superposition, entanglement, etc., enabling many new properties that sometimes seem to fall more in the realm of fantasy than fact. For example, quantum entanglement has been successfully demonstrated over many kilometres: particles are linked and correlate in the same state although there is no connection except in the quantum plane.

In practical terms, this means that quantum computers can solve some problems (e.g. optimisation, shortest path) in a single operation, rather than trying all possibilities through iteration, as we do now. For example, the polynomial-time quantum algorithm developed by Shor can be used to determine the prime factors of a large number in a fraction of the time required by conventional means. Factorisation (trapdoor algorithms, easy in one direction—multiplication—and hard in other directions) is one of the possible options for all PKI security<sup>60</sup>. For security applications this means that RSA<sup>61</sup> encryption (the basis for absolutely everything today: secure web communication, all encoding, authentication, encryption, chips, etc.) is broken. All our previously secure systems, which it would now take centuries to crack with the biggest supercomputers, become open. There is some way to go to make this a practical reality, but some serious commentators see this as coming sooner rather than later.

It is therefore more important than ever to rethink our current protection mechanisms, develop a plan for the quantum world and take advantage of opportunities for even better security afterwards (e.g. quantum cryptography).

---

<sup>60</sup> Shor’s theorem can be used to solve the hard problems that are leveraged by asymmetric ciphers (integer factorisation, computing the discrete logarithm, multiplication on an elliptic curve) in polynomial time if quantum computers are available.

<sup>61</sup> Or more generally *asymmetric cryptography*, since it is not only RSA that is vulnerable to quantum algorithms. The security community is currently heavily researching post-quantum cryptographic algorithms.

### 3.6.1.2.10 Data Breaches

Since we have very poor digital identity checking on the one hand that is typically based on password technology from the 1970s, and an increasingly professional and industrialised hacking industry on the other, the number of data breaches is exploding.

The prizes are getting bigger as the world moves all services in all industries to digital. Thus, identity theft, used for breaking into online banking, ATMs, card infrastructures, web accounts and virtual wallets, is becoming increasingly rewarding<sup>62</sup>. Banks are holding up quite well in this field, but even some of them have been compromised (see above fraud overview filtered for only financial service frauds).

Certainly, some industries close to banking have experienced massive hacks and data leaks (for example, Equifax<sup>63</sup>), but this is not the norm as it is in other industries. For companies like Yahoo, which repeatedly lose billions of accounts, being hacked is almost business as usual. See snapshots<sup>64</sup> for some of the more recent examples where hundreds of millions of accounts are exposed at a time. It really is time to put a stop to this if we want to move further into our digital world.

### 3.6.1.3 The Good News

#### 3.6.1.3.1.1 Regulatory Clarity

The first good news is that a good number of questions posed by the Open Banking community on details of regulation have been answered. The EBA, which was tasked to define the detailed RTS regulatory technical standards, has put up a Q&A tool<sup>65</sup> and has answered many questions for market participants. In addition, the market players themselves have increasingly managed to determine, in dialogue with regulators and employing many lawyers, which implementations will be compliant and useable. This also ensures that the consent will be meaningful, unlike the current GDPR consent pop-ups.

Examples are a year-long exercise by Visa, where all aspects of secure customer authentication have been defined<sup>66</sup>, including all the many niche use cases. For example, how to:

- make SCA-compliant payments offline (!) at the duty-free cart in an airplane<sup>67</sup>;
- pay for your hotel at booking.com, where, surprisingly, the hotel owner typically types in the payment details manually at his front-desk POS terminal – the card details entered at booking.com are mostly not processed automatically;
- pay with multiple factors using a games console/smartTV/watch/car<sup>68</sup>

Getting good/compliant authentication and informed customer consent in a legal and acceptable way is very difficult under the regulatory boundary conditions. However, it looks as though all key players have now –

<sup>62</sup> <https://www.marketwatch.com/story/identity-theft-is-skyrocketing-and-getting-more-sophisticated-2018-02-27>

<sup>63</sup> <https://www.bbc.co.uk/news/business-41192163>

<sup>64</sup> For example, <https://www.securitymagazine.com/articles/91366-the-top-12-data-breaches-of-2019>

<sup>65</sup> <https://www.eba.europa.eu/single-rule-book-qa>

<sup>66</sup> <https://www.visa.co.uk/partner-with-us/payment-technology/strong-customer-authentication.html>

<sup>67</sup> [https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019\\_4740](https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4740)

<sup>68</sup> For example, [https://help.twitch.tv/s/article/updating-payment-information-transaction-history?language=en\\_US](https://help.twitch.tv/s/article/updating-payment-information-transaction-history?language=en_US)

after many months of work and alignment – found a way through. Amazon were to deploy two-factor authentication in December 2020 (ahead of the regulatory deadline of 1 January 2021) and they will surely have ensured that there will not be any cart abandonments due to poor implementation for Christmas shoppers<sup>69</sup>.

In addition, security researchers may also have ideas on how to further improve the authentication process, making it smoother and more secure.

### 3.6.1.3.2 B2B

The focus on B2B in Open Banking continues to be strong and dominant, which is good news, as that is where the real difference can be made. That is where the huge industrial processes lie, where added efficiency and functionality will be a real benefit and where real business cases are much more easily made. The consumer business – unlike corporates, consumers do not pay for making payments – is much more difficult. Moreover, banks traditionally do not serve their corporate clients well, leaving much opportunity for nimble new entrants.

Hence, in practice we can see that the majority of new FinTechs do not serve the consumer space but instead position themselves as B2B technical providers to banks and corporates wishing to use Open Banking more effectively. There are a number of new players that not only serve existing industry, but are putting up B2B propositions in their own right to make new advanced treasury services (“Treasury 4.0”) possible, optimise capital management, improve bill reconciliation, improve lending, etc. Although Open Banking was originally proposed as a consumer proposition and is often spoken about as such, the focus is now firmly on B2B. That, after all, is where the money is.

Accordingly, security research should focus on this area, as it is the main attention point of FinTechs and where the largest money flows are.

### 3.6.1.3.3 Instant

There is a massive drive towards “instant” payments, with some interesting “smart POS” models emerging. SmartPOS means that customers will receive a much richer functionality at checkout than just “sticking their plastic card in” (really or virtually). Customers at a smartPOS will not only be able to pay, but will be offered financing, FX service, options to pay from their savings account and much more.

The instant payment proposition (where the money arrives in the payee’s account not a day or so later, but in seconds) is sweeping the world. This is good news for everybody, especially in the real-time eCommerce world.

There will, however, be some challenges for real-time security checks: AML<sup>70</sup>-checks, ATF<sup>71</sup>-checks, FATF<sup>72</sup>-checks, limit-checks will now need to be done in real time and with the same accuracy and better

---

<sup>69</sup> Security vs cart abandonment has long been a conundrum for online payments. See:

<https://seon.io/resources/minimize-checkout-abandonment-rates/> and

<https://nakedsecurity.sophos.com/2019/06/10/online-shops-fear-2fa-at-checkout-will-increase-abandoned-carts/>

<sup>70</sup> Anti-Money Laundering

<sup>71</sup> Bureau of Alcohol, Tobacco, Firearms and Explosives (<https://www.atf.gov/qa-category/national-instant-criminal-background-check-system-nics> )

<sup>72</sup> Financial Action Task Force (<https://www.fatf-gafi.org/> )

false positive rates. Good for B2B but worrying from a fraud point of view is that the limit per transaction has been raised to 100,000 €, despite the lack of any experience of fraud development following the wide-scale deployment of instant payment methods. With instant, the money is also gone immediately (and irrevocably)!

The UK market, where “faster payments” were introduced over a decade ago, demonstrated that fraudsters are quick to exploit new “instant” fraud schemes, leading to huge losses, e.g. £354m in 2018. Some remedies have been put in place, notably payee identification, to combat push scams but there is still a need to look more closely at security mechanisms for instant in Europe.

This is especially urgent, since the ECB and Commission are applying a massive push to get all of Europe on instant as fast as possible. Currently, a little over half the European banks are instant-ready but the usage is still low (<8% of volume), partly because some banks are trying to charge extra for instant payments which will not be accepted by the market. Thus, the current rapid introduction of “instant” payments will lead to new instant fraud models that will need to be counteracted.

The high volumes (all transactions in Europe) and high limits (up to 100k€ per transaction) will make this a honeypot for fraudsters. Creative solutions for mitigating the threat will be welcomed heartily by banks, merchants and consumers.

#### **3.6.1.3.4 Open Banking Fraud**

One of the best pieces of news is that there have not (yet) been any major reported cyber breaches based on Open Banking. The lack of Open Banking fraud may be due to the slow pace of development of Open Banking itself, especially in Europe. The fraudsters are waiting for all banks to be easily accessible.

The UK has forged ahead, with a complete scheme, a tight API standard, an OBIE app store model, and half of EU FinTechs in the UK), whereas Europe is still bogged down in technical discussions around API standards, and a pan-European data access “scheme” is as far away as ever. However, this scheme has now be delegated from the European Retail Payment Board (ERPB), after having been with them for more than two years to the European Payments Council (EPC), which will benefit from being multi-stakeholder.



Figure 5: Overview of elements of API scheme <sup>73</sup>

At present we just have APIs. However, we also need refund methods, structured dispute resolution (instead of many people calling a hotline or sending an email), standardised customer journey guidelines (to assure a minimum quality of user experience), automated FinTech onboarding (instead of connecting each FinTech manually to each bank), etc. – see Figure 5 for a general API scheme overview. This has been largely achieved in the UK, but not in Europe. Once we have the complete solution and scheme (and not just some APIs) we must be prepared for Open Banking to take off.

Meanwhile, we can be sure that the hackers already have their own Open Banking projects in the pipeline and are focusing on where they will aim to attack. Open APIs with shared data will give them a broad attack surface. It is important – and this may be a key topic for CyberSec4Europe – to anticipate and propose countermeasures.

### 3.6.1.3.5 Data

One of the biggest initiatives of the new Commission is that it has published a whole slew<sup>74</sup> of documents (A European Strategy for Data<sup>75</sup>, Data Governance in Europe<sup>76</sup>, Retail Payment Strategy<sup>77</sup>, Financial Services Strategy<sup>78</sup>, Data Act, etc.) that are pushing the banking industry – and now also other industries – into wider data sharing and hence new security challenges.

The challenges posed by Open Banking (*only* two APIs, for data access and payment initiation, were mandated, and *only* for banks) will be catapulted into an entirely new dimension, as all industries will be required to share all data (subject to many governance restrictions, of course).

<sup>73</sup> Source: M. Salmony, published since 2014, above diagram updated from <https://informaconnect.com/payments-international/speakers/michael-salmony/>

<sup>74</sup> <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy>

<sup>75</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066>

<sup>76</sup> <https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-data-governance-data-governance-act>

<sup>77</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0592>

<sup>78</sup> [https://ec.europa.eu/info/publications/200924-digital-finance-proposals\\_en#:~:text=The%20strategy%20sets%20out%20four,including%20enhancing%20the%20digital%20operational](https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en#:~:text=The%20strategy%20sets%20out%20four,including%20enhancing%20the%20digital%20operational)

This is a very fruitful field for security researchers to see how a wider “data market” across all industries and all data sources can be set up securely.

#### **3.6.1.3.6 Blockchain**

While the hype around Bitcoin has largely died away, it does continue to play a significant role for speculators (with entry costs currently at USD 50,000) and for criminals.

For criminals, Bitcoin is a useful way of collecting funds, since this “currency”, although electronic, is fairly anonymous. Thus, ransomware can be collected without too much fear of being traced and caught and without concern about measures against money laundering, terror financing, etc.

One of the most successful attacks (WannaCry in 2017<sup>79</sup>) hit more than 200,000 computers across 150 countries, including some in the UK’s NHS in MRI scanners, blood-storage refrigerators and operating theatre equipment<sup>80</sup>, with global damages reaching billions of dollars. The ransom money is exclusively collected in Bitcoin.

Closer to our topic, ransomware also sometimes impacts the banking industry, for example in the case of Sopra Steria<sup>81</sup>.

The good news is thus that after ten years of massive hype, expectations and investments, the buzz around Bitcoin has died down significantly. However, its use for speculation (due to massive volatility/instability) and crime (due to anonymity) continues.

Some security specialists see blockchain (the underlying technology behind Bitcoin and other cryptocurrencies) as having the potential to provide better payment and security.

#### **3.6.1.3.7 eIdentity**

The EU is at last placing more emphasis on eIdentity, recognising that reliable identification – who the connected parties are and what attributes and rights they have – must be the basis for all digital services. Using 1970s technology like passwords (as is still highly prevalent today) will mean that all digital services will be built on sand<sup>82</sup>.

Since Europe’s flagship identity project eIDAS (electronic identification and trust services) is proving to gain limited traction even in the public sector, one can sense a reset in the thinking by the Commission on the best approach towards digital identity. This is already apparent with the proposals for an EU ID wallet. The future is not only in government-issued identity but will be in a federated approach where attributes of people and things are verified.

Security research can and should contribute to how to set up a reliable cross-industry identity infrastructure that can provide a solid basis against identity theft and online banking attacks (often based on gaining the credentials, i.e. the identity, of the target).

---

<sup>79</sup> [https://en.wikipedia.org/wiki/WannaCry\\_ransomware\\_attack](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack)

<sup>80</sup> <https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/#:~:text=On%20Friday%2012%20May%202017,been%20attacked%20before%2012%20May>

<sup>81</sup> <https://www.finextra.com/newsarticle/37020/sopra-steria-to-take-multi-million-euro-hit-on-ransomware-attack>

<sup>82</sup> The Age of Consent, The Case for Federated Bank ID, Citi - <https://www.citi.com/tts/insights/articles/article77.html>

### 3.6.2 SWOT Analysis

A summary of the Open Banking SWOT analysis is presented in Figure 6. Detailed SWOT analysis results are presented below.



Figure 6: Open Banking SWOT Summary

#### 3.6.2.1 Strengths

- The EU has taken the lead in planning and legislating for the next generation of finance, embracing customer and corporate banking as well as payments, through a series of regulations and directives that include PSD2, AML5, the GDPR and eIDAS. Furthermore, the EU's Digital Finance Plan published in 3Q2020 is aimed at promoting common technical API standards and going beyond the scope of PSD2.
- Although the implementation of Open Banking has had a slow start since it was introduced in Europe, the benefits are being realised in contexts and partnerships that five years ago would have seemed improbable. For example:

- Marcus – the online bank from Goldman Sachs – partnering with Saga to offer savings accounts<sup>83</sup>
- CYBG and Go Compare partnering for energy switch services in the price comparison world<sup>84</sup>
- consumer brands such as the AA partnering with the personal loan marketplace platform, Monevo<sup>85</sup>
- in the US, the bank Wells Fargo & Company entered into a data exchange agreement with Envestnet | Yodlee, a leading financial data aggregation and analytics platform<sup>86</sup>

These strategic partnerships allow both parties to achieve greater scale and improve customer reach, while satisfying consumer requirements in a cost-effective manner.

### 3.6.2.2 Weaknesses

- The very things that underpin the EU’s strengths also expose its weaknesses: i.e. in addition to opening up the market for payments to a whole range of new actors, PSD2 has also opened up a can of worms in terms of liabilities, directly relating to financial fraud and data loss, but also with the knock-on impact of damage to brand reputation.
- Another weakness is that PSD2 is “only” a directive, not a piece of legislation, which means that it can be (and is being!) interpreted differently by different Member States, as well as independently by banks themselves. There are too many in Europe tasked with ensuring that the new standards are coordinated. Leaving it up to the market has resulted in a balkanized set of implementations across Europe.
- There are fears and challenges associated with introducing open banking, amongst which implementation headaches are probably the most challenging, both in terms of cost and disruption, closely aligned with ensuring adequate security. The myths that deployment costs are unaffordable are not without foundation. Compliance in a regulatory-driven environment is an anticipated consideration but, provided the rules are clear, it is not a real barrier. Another concern is that competitors will steal customers but this is not a factor specific to open banking.
- A further concern comes from some banks mistakenly claiming to support open banking when only using internal APIs or bespoke private APIs (for example, to connect to Visa or specific FinTechs). Partner banking is clearly not open banking. Going beyond this, some banks<sup>87</sup> have introduced a developer portal or API marketplace that allows any third-party developer to use the APIs a bank has developed

### 3.6.2.3 Opportunities

<sup>83</sup> <https://www.retailbankerinternational.com/news/saga-goldman-sachs-marcus-roll-out-two-savings-products/>

<sup>84</sup> <https://www.insider.co.uk/news/cybg-industry-first-energy-switching-18211702>

<sup>85</sup> <https://www.fairinvestment.co.uk/aa-car-loan/>

<sup>86</sup> <https://www.businesswire.com/news/home/20200924005156/en/Wells-Fargo-and-Envestnet-Yodlee-Sign-Data-Exchange-Agreement>

<sup>87</sup> For example, Nordea: <https://developer.nordeaopenbanking.com/> and <https://www.openbankingtracker.com/provider/nordea>

One of the stark realities of the 21<sup>st</sup> century for traditional banks came with the global financial crash in 2008. This had a significant impact particularly on young people, who have been struggling ever since with multiple financial challenges, including the increase of house prices, the rise of the gig economy and lower comparative wages.

- As a consequence, millennials but also other demographics have been seeking new and innovative financial products to help them manage their finances against a background of lack of savings and rising debt. In addition to the demise of physical high street banks<sup>88</sup>, the growing reliance on mobile devices has attracted younger generations to digital-only challenger banks, such as Monzo, Revolut, Starling, which have been able to focus their investment on tech and partnerships to provide a range of products marketed specifically to cost-sensitive digital natives, with brightly-coloured bank cards and user-friendly modes of customer communication that traditional banks struggle to emulate. In addition, millennials value – and expect – services that are convenient and simple.
- In areas that the major banks tend to ignore, serving those who are underbanked, struggling to manage their money or building credit scores, FinTech innovation will continue to disrupt the banking sector.

#### 3.6.2.4 Threats

There are several threats, not so much for the financial community as a whole, but for the Open Banking initiative itself:

- (1) Outstanding gaps in security in financial transactions introduced with Open Banking that are still being resolved.
- (2) Poor communication of the benefits to the general public: “openness” and “banking” or “financial transactions” are not words that sit comfortably together unless explained very clearly, succinctly and in non-technical language. For example, in a survey carried out in the UK 12 months after open banking was launched<sup>89</sup>, adult UK consumers were interviewed to gauge their awareness, understanding of benefits, and security concerns that could affect growth. The study found that 78% of UK consumers lacked awareness of the existence of open banking and some perceived that “open” banking implied a lack of security. However, it would not be unreasonable to conclude that this highlights the difficulty of assessing the value of surveys – so much depends on who is asking the questions!<sup>90</sup>

---

<sup>88</sup> It is projected that in the UK high street branches will no longer exist by 2032 -

<https://www.asktraders.com/analysis/bank-in-crisis/>

<sup>89</sup> Unlimited Group *Open banking: a revolution stalled*. (second edition): [https://www.unlimitedgroup.com/wp-content/uploads/2018/12/LG-Unlimited-Open-BankingReport\\_Splendid\\_v03\\_LR.pdf](https://www.unlimitedgroup.com/wp-content/uploads/2018/12/LG-Unlimited-Open-BankingReport_Splendid_v03_LR.pdf).

<sup>90</sup> A far more credible and detailed scientific analysis was carried out by the ECB based on a survey in the Netherlands in 2019: [The impact of PSD2 on the functioning of the retail payment market](#), Michiel Bijlsmaa, Carin van der Cruijnsena, Jakob de Haana, and Nicole Jonker. A more specific sectoral report from 2020 is: [The impact of Payment Services Directive 2 on the PayTech sector development in Europe](#), Michał Polasik, Agnieszka Huterska, Rehan Iftikhar, Štěpán Mikula

- (3) Banks may conclude that the risks associated with open banking, in terms of both the threat of data loss and financial fraud, may make it so unattractive that they adopt approaches to make it difficult for AISPs/PISPs to collaborate with them – a clear example would be the adoption of singular APIs.
- (4) It was initially thought that the ultimate approach to kill the FinTech revolution would be through mergers and acquisitions: if banks were to feel sufficiently threatened, acquiring an upstart start-up or challenger would be one way of keeping a tight control on emerging trends. Fortunately, the reality is that traditional banks are finding ways to collaborate with FinTechs to achieve mutual benefits – so much so that a lot of banks are buying up FinTechs and FinTechs themselves are merging. Both trends are really positive indicators of the overall currency of Open Banking, although only time will tell.
- (5) As mentioned above, there is still no unanimity on the structure of the open APIs adopted by banks across Europe. Although this is not a total inhibitor, unless resolved with a degree of compatibility/interoperability, there will continue to be a fractured open banking landscape across Europe – and beyond.
- (6) Following the concerns raised below in considering European Digital Sovereignty, it is not beyond the realms of possibility that a global industry-driven initiative, emerging, say, from the US, could coalesce around a common API – such as for example the OpenID Foundation’s FAPI (financial-grade API) – that would leave Europe apparently out of step with the rest of the world unless it followed suit.

Nonetheless, although FAPI has powerful advocates, there are numerous global or international Open Banking API standards being worked on including:

- The Open Banking (OBIE) working group
- US FDX
- ISO / TS 23029:2020
- W3C
- SWIFT
- UPI (ISO 20022)
  
- There are multiple European PSD2 standardisation initiatives, of which the Berlin Group is by far the most used, with 78% of banks across 20 countries and going global, with Israel, Russia, Iceland and others expected to follow suit.

### 3.6.3 European Digital Sovereignty

As with most major industries, banking and payment services are a global phenomenon, and it would be very difficult – as well as unrealistic and undesirable – to isolate one region from the rest of the world. With that in mind, it is salutary to consider that, while Europe is seeking to resolve the knots with the implementation of PSD2 and Open Banking, the rest of the world is not waiting to see the result. Although banking authorities in the rest of the world are as fragmented as they are in Europe, developments elsewhere in the industry have the potential to undermine the lead taken and the subsequent progress made in Open Banking in Europe – see Table 1 for a comparison of Open Banking initiatives worldwide.

As stated above, Europe has a global lead in the development of Open Banking regulation and now has to strive to achieve harmonisation across the region. One of the major struts in Europe's advance on the path of digital sovereignty will come with the full realisation of its Digital Strategy, which will both increase the adoption of Open Banking and make use of significant contributions from it.

Table 1: Open Banking global comparisons

Country	Approach	Mandate Authority	Open Banking Framework Release Date	Other	Example
<b>Singapore</b>	Market-driven	Monetary Authority	2016 - API Playbook released in cooperation with the Association of Banks	Voluntary adoption by FIs.	In 2017, DSB Bank launched its largest API developer portal with more than 155 APIs available.
<b>Hong Kong</b>	Market-driven	Monetary Authority	2018 (January) Published Open API Framework	FIs decide which TPPs to collaborate with using bilateral agreements.	HKMA launched Open API on its website in July 2018. Approximately 130 sets of information covering financial data and other banking information were made available for Open API by phases, including statistics on HK dollar exchange rates, interest rates, the banking sector and the Exchange Fund, as well as press releases and Coin Cart schedule. Stakeholders and consumers can use the information for research or to develop new applications.
<b>China</b>	Market-driven			Driven by big tech companies Tencent and Ant Financial.	When a consumer/small business applies for a loan on Ant Financial's Mybank, the loan is automatically offered to one or multiple FIs across an API.
<b>Japan</b>	Regulatory	Banking Act	2018 – Revised Banking Law (2017 initial release) <ul style="list-style-type: none"> <li>• 2018 amendments set requirements for FI/FinTech partnerships to formalise registration rules, standards, and development of open API systems by June 2020</li> </ul>	80% of FIs must have APIs in place by 2020.	Mitsubishi UFJ Financial Group is providing TPPs secure access to its databases as part of its Open Banking projects
<b>Brazil</b>	Regulatory	Monetary Authority	In four stages between November 2020 – May 2022 <sup>91</sup>	Brazil is the largest FinTech market in Latin America – fifth in the world - with	Ozone Global Sandbox to be used in the run up to Brazil's full market implementation of Open Banking as a space to test and develop proof of

<sup>91</sup> The implementation will occur in four phases:

- **Phase I:** Access to information from the participating institutions regarding customer service channels, in addition to products and services related to deposit or savings accounts, payment accounts or credit operations. This phase is already in place up to February 2021.
- **Phase II:** Sharing of customers' registry information and transactional data related to the products and services listed in Phase I, started in August 2021.
- **Phase III:** Sharing of payment transaction initiation services and forwarding loan proposals, started in October 2021, this phase will be set up gradually until 2022.
- **Phase IV:** Expansion of the scope of data covered, including foreign exchange operations, investments, insurance, and more. This phase will start in December 2021 (for products and services), making Open Banking fully operational (for customer transactions) in Brazil by May 2022.

The major banks in Brazil – will be forced to adopt open banking, although all authorised institutions can adopt, as long as they comply with reciprocity and share information.

				about 400 companies. Investment in Brazilian FinTech companies totalled about USD52 million in 2015, reaching USD 1.6 billion in 2019	concepts in collaboration with TecBan, an established multi-bank and multi-access platform
<b>Australia</b>	Regulatory	Customer Data Right (CDR) legislation	2019 (August) <ul style="list-style-type: none"> <li>• CDR gives customers control of their data and enables them to share it with third-parties (similar to GDPR)</li> <li>• Data Standards Body (DSB) – lays foundation for cross-industry data sharing</li> </ul>	Top four FIs must comply by February 2020. Smaller FIs must comply by February 2021.	No examples available.
<b>New Zealand</b>	Market-driven	Payments NZ (government-owned)	2018 – API Pilot Program announced by Payments NZ with six participants: ASB, BNZ, Datacom, Paymark, Trade Me, and Westpac (FIs and TPPs)	Development and testing of new API specifications over a five-phase process.	The “Jude” app allows users to link all their bank accounts to its platform, enabling account management through a single digital portal.

### 3.6.3.1.1.1 A Pan-European Approach

The European Parliament is putting increasing pressure on banks to create a harmonised continental scene. All other major domains (Russia, China, US, etc.) have their own continent-wide harmonised payment scheme – in Europe instead we have massive fragmentation, for example:

- the very successful iDeal in the Netherlands can hardly be used outside the Dutch borders;
- the German girocard, the use of which is surging, cannot be used abroad;
- very successful Nordic payment apps, like Vipps in Norway, Swish in Sweden or MobilePay in Denmark, cannot be used outside these Nordic countries.

All these national successful solutions are gaining further traction and thus have become more entrenched because of COVID-19. Demand for contactless payment (in the form of the local girocard) instead of cash handling has even reached (previously notoriously cash-oriented) Germany and is proving a winner that is here to stay.

This European fragmentation is a unique downside for our continent. By contrast, there are no local schemes in the US – one can pay the same way in California as in Wyoming. This local fragmentation threatens European sovereignty (since all international schemes used here are provided by American Visa/Mastercard/AmEx/PayPal and increasingly Asian AliPay, etc.).

The only way to pay in all European countries is with Euro banknotes or with a US-branded card or Chinese app.

This has motivated the regulator to force banks into developing a pan-European payment scheme. Banks have created the EPI (European Payment Initiative) to respond to this, but debate on whether this will be successful, and whether it will be based on Open Banking (as it should be), is still open. In any case, any

security solutions proposed should ideally be independent of instrument and local method, and should be applicable Europe-wide.

## CBDC

The regulator has more or less openly put enormous pressure on the banks, saying: if you do not stop this nationalistic approach (see above) then we will ask the central bank to issue its own pan-European currency (CBDC<sup>92</sup>) in competition with commercial banks<sup>93</sup>.

Many market observers expect CBDC to be inevitable (see Lagarde<sup>94</sup>).

This is not a technological topic (and it will not be based on blockchain, since it needs to be hugely scalable, energy efficient, private, work offline) but a deeply political project threatening the core position of the banks (their loans and deposits, their ability to create money – many find it surprising that only 5% of all money is created by the central banks) with deep consequences for monetary policy (interest rates), sovereignty (vs. Chinese electronic central bank money which is already well progressed) and for the future of cash.

This is a topic to keep in focus, to see whether it will come, and if so, what security issues this will raise.

### 3.6.4 COVID-19 and Public Health Dimension

Depending on who you ask or which way you look at it, COVID-19 has either provided a great opportunity for Open Banking or has exacerbated the risks.

As we saw earlier (see girocard example), COVID-19 has caused a massive push towards digital services (e.g. contactless payments +15%, now 75% of all accounts in Europe are contactless enabled – and the limit has been raised, often doubled, in Australia even to \$200 per transaction). This provides for better convenience and more acceptance, but it has also increased the attack surface<sup>95</sup>.

#### 3.6.4.1 Opportunities

The pandemic has re-emphasised the value of APIs in the commercial banking space. API-driven systems are enabling faster payments, as well as providing clear working capital and operational benefits to businesses facing COVID-related cash-flow pressures. They are also being used to deliver new propositions that help companies boost their competitiveness in crowded marketplaces and improve their customer experience.

---

<sup>92</sup> Central Bank Digital Currency

<sup>93</sup> Note by the ECB for the Economic and Financial Affairs Council  
<https://www.ecb.europa.eu/pub/pdf/other/ecb.other191204~f6a84c14a7.en.pdf> : “If industry efforts fall short of developing an innovative and efficient pan-European payment solution, the social need for it could potentially be met by issuing a CBDC”

<sup>94</sup> <https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200910~31e6ae9835.en.html> “we know that the private sector, by contrast, has made far less progress on delivering a pan-European solution for retail payments.”

<sup>95</sup> Heightened online spending will cause fraud to increase at an exponential rate, LexisNexis, November 2020

COVID-19 has emphasised the need for businesses to have strong insight into their operations, by taking a granular look at the data locked in systems and supply chains to gather information they can act on amid complex trading conditions. Open Banking APIs are helping businesses better understand their financial position by enabling greater access to their own banking data. For example, Lloyds Bank Commercial Banking is testing an intelligent bookkeeping solution that combines Open Banking data with other operational data, such as invoices and expenses, thereby reducing the administration load for small and medium businesses and enabling them to make better financial decisions through real-time cash forecasting and profit and loss information.

Retail and hospitality, the sectors most adversely affected by pandemic restrictions, have by necessity had to move away from the use of cash in transactions. This has provided new opportunities for the deployment of tech-enabled payment systems, particularly concerning solutions that support social distancing and help businesses manage overhead costs.

This includes options such as pay-by-bank, which allows customers to pay merchants directly through their banking app. Pay-by-bank supports merchants' working capital by providing fast payment settlement, and removes the cost of card transaction fees, thereby helping to reduce overheads. Other solutions, such as pay-by-app and pre-ordering systems, also have a role to play, and as the impact of COVID-19 continues there is opportunity for further innovation and new propositions from both FinTechs and financial institutions, including mutually beneficial partnerships. For example, Validis, a cloud-based FinTech, helped streamline Santander UK's SME loan monitoring process by providing real-time API data feeds that accessed granular Management Account data to automate loan covenant monitoring for SME clients<sup>96</sup>. During the pandemic, the benefits of speeding up loan application processing through the UK Government's Coronavirus Business Interruption Loan scheme helped struggling smaller businesses stay afloat.

Not surprisingly, major banks, asset and wealth management firms, insurers and intermediaries responding to the latest Lloyds Bank Financial Institutions Sentiment Survey cited APIs as one of their top three tech investment areas in the year ahead, along with cybersecurity and the cloud<sup>97</sup>.

#### 3.6.4.2 Threats

A threat to one person can be an opportunity for another. The opportunities for Open Banking that have arisen as a result of the pandemic also have the potential to accentuate the risks and security challenges that existed before March 2020. Fraudsters love disruption and thrive on exploiting other people's challenges.

---

<sup>96</sup> <https://www.validis.com/wp-content/uploads/2019/08/SantanderCaseStudy2019.pdf>

<sup>97</sup> Financial Institutions Sentiment Survey 2020: Looking beyond lockdown, 25 September 2020  
<https://www.lloydsbank.com/business/resource-centre/insight/financial-institutions-sentiment-survey.html>

*“Technology remains the top investment priority for the UK financial services sector as firms seek to drive efficiency, improve customer experience and grow market share in an increasingly competitive environment. Cybersecurity, the cloud and Application Programming Interfaces (APIs) lead the way in investment priorities for firms. Interestingly, the excitement around blockchain acquisition has faded since 2019, quite possibly signifying firms' aims to embed and drive value from previous investments.”*

Not surprisingly, there has been a significant increase in all forms of fraudulent activity across all business sectors during the pandemic. The criteria are common and well-known: people working from home instead of the office, whilst juggling childcare and worrying about finances and the future; businesses with worries over cash flow and revenues having to apply for emergency loans or government-backed support.

Personal and corporate banking customers have been targeted by fraudsters through a significant spike in malware, phishing emails and social engineering approaches. Banks have had to work proactively to raise awareness and to provide guidance on the basics of good security.

Banks' employees working from home are equally susceptible to phishing emails and other scams. The threat is exacerbated when multiple family members log in on the same network and click on links and content of many different kinds, potentially exposing devices to malware that could then enter a bank's system if the right endpoint controls are not in place.

Banks have sophisticated and established connectivity and IT systems and already enable many staff to work remotely when needed, but were not prepared for the huge jump in employees at all levels needing remote access on a daily basis. Some staff may lack the hardware or software needed to access a bank's VPN, leading to IT teams loosening some controls in the short term.

COVID-19 has created a huge monitoring challenge for many sectors (for example, education) and, although online banking and payments were well-established before the pandemic, the financial sector has been impacted, as is evidenced by:

- Growth in transactions recorded from new devices not seen before in the Digital Identity Network
- Growth in new online banking registrations for several financial services organisations
- A spike in new account creation for financial service organisations
- Evidence of fraud targeting COVID-19-related support packages across several financial service organisations
- Evidence of an increase in identity spoofing and first party fraud targeting some e-commerce merchants.<sup>98</sup>

Banks, like many other businesses, need to ensure that remote users are who they say they are, and that their online behaviour is consistent with what is expected. This is difficult when users may be logging in not only from company-issued laptops but also their personal phones, tablets and other devices. Usual BYOD protocols that allow remote access only from one device may have been relaxed. In addition, employees are most probably not following their usual work patterns but may be working in bursts across different hours as a result of childcare and other duties.

Because of lockdowns, banks are expanding the range of self-service options available to customers online – for wealth management trades, mortgages, loan applications, etc. Ensuring robust security controls are in place over this new customer functionality becomes even more essential. For example, the regulatory rules associated with trading require that calls with traders are recorded and monitored, arrangements that become

---

<sup>98</sup> The LexisNexis® Risk Solutions Cybercrime Report January-June 2020 <https://ccstatic.ccindex.cn/event/24/51/85/3/rt/1/documents/resourceList1599860038487/lexisnexisrisksolutions/cybercrimereporth120201599860034880.pdf>

precarious when traders are working from home. Regulators have allowed some short-term leeway, given the importance of keeping liquidity flowing in the marketplace, but it is not sustainable for long.

Post-COVID-19, with levels of remote working likely to remain higher than they were pre-COVID-19, banks may need to reset some of their protocols and policies around access management, finding ways to increase flexibility without compromising security. Needless to say, all banking operations, and new and innovative ones in particular, will require strong information security, cyber and anti-fraud controls. All of these could create a more conservative approach to Open Banking in 2021.

### 3.6.4.3 Beyond COVID – the public health dimension

Open Banking is being used to address health issues, particularly in relation to improving mental health. According to the UK's NHS,<sup>99</sup> one in four adults and one in 10 children experience mental illness, and there are probably many more that are known or being cared for who are not on the public radar – which would account for 13 million people in the UK alone. Using Open Banking apps developed as part of one of its challenges, OB4G (see section 3.6.7 below) reports that 75% of alerts signalled that daily spending thresholds had been reached.<sup>100</sup> User participants, who were willing to open up about their finances in a way not seen before, also benefitted from practical help with money and built better financial habits. By being able to access a clear, accurate picture of their overall finances, 10 out of 21 users surveyed said that they had to spend less time budgeting or managing money, that they borrowed less and that they saved more each month – all of which resulted in less struggle to make ends meet and a general reduction in income and expenditure fatigue that in turn may lead to better outcomes for individuals and consequently reduce money-related anxiety.

#### 3.6.4.3.1 Mental Health

According to the BBC, 30% of us will struggle with mental health at some point in our lives (November 2019),<sup>101</sup> and, shockingly, suicide is the single biggest killer of men under the age of 45 (March 2019).<sup>102</sup> The affected person, their doctor and their carer can be helped with data – not only health- or social media-related data but also financial data. Is the person suffering from financial stress, do they have a large debt or overdraft, are they having to pay late payment fees, are they defaulting on loans and, just as significantly, are they consuming an excessive amount of alcohol or drugs? This is an extremely sensitive topic and involves very sensitive data, and only time will tell whether patients/society will accept what could be perceived as intrusive. If they do, there is a large potential for improving patients' care and for reducing the burden on health services.

---

<sup>99</sup> <https://www.england.nhs.uk/mental-health/>

<sup>100</sup> Open Banking For Good: Making A Difference? Sharon Collard and Jamie Evans, March 2021

[https://static1.squarespace.com/static/5b3b35d95b409b6cfd1c9ad6/t/6076c1779a3ed37d3799555e/1618395546708/OB4G\\_Making+a+difference.pdf](https://static1.squarespace.com/static/5b3b35d95b409b6cfd1c9ad6/t/6076c1779a3ed37d3799555e/1618395546708/OB4G_Making+a+difference.pdf)

<sup>101</sup> <https://www.bbc.co.uk/sounds/play/w3csytgz>

<sup>102</sup> <https://www.bbc.com/future/article/20190313-why-more-men-kill-themselves-than-women>

### 3.6.4.3.2 Gambling

As many as 22% of UK online gamblers using credit cards are recognised as “problem gamblers”, some of whom have accumulated tens of thousands of pounds of debt through gambling because of credit card availability. As a result, the UK’s Gambling Commission banned the use of credit cards for all gambling services from 14 April 2020.<sup>103</sup>

Account-based payments can help. Open Banking’s Payment Initiation Services (PIS) allow service providers to create new payment solutions that will allow the initiation of payments and financial transactions. This can lower the cost of making payments, as they are made directly from bank account to bank account, and increase convenience. For gamblers, this would involve the immediate debit of stake money with no danger of going beyond the account limit, and, at the very worst, they might attract bank overdraft fees which are not in the order of credit fees that are typically about 20% APR. The gambling industry would also welcome direct account-based payments as this would massively reduce the fraud chargebacks that are so prevalent in this industry.

### 3.6.5 Green Deal and Climate Change

Europe is a leader in Open Banking and aims to be a pioneer of a data-led economy based on open finance. The recently published European Data Strategy includes open finance and suggests recommendations rather than prescribing regulations, with the objective of creating a policy environment by 2030 in which open data can thrive on improved standards, infrastructure and data availability.

The main drivers for the open data vision are to establish Europe as a global market leader in data and to foster the European Green Deal. To meet the goals of becoming carbon neutral by 2050 and more competitive, the Member States are expected to invest in data openness in multiple industries through data literacy, artificial intelligence, cloud, blockchain and IoT. Access to data, which is at the core of Open Banking, will be key to this ambition.

*It will be important to ensure that across the EU, investors, insurers, businesses, cities and citizens are able to access data and to develop instruments to integrate climate change into their risk management practices.<sup>104</sup>*

Through what might be heralded as “Open Banking for Carbon”, it is possible to calculate your footprint and guide lifestyle and other choices with data.<sup>105</sup>

As 70% of emissions are caused by individual consumption (what and where we eat; how often and how far we travel and by what means), the first step is to let individuals understand how their daily decisions affect their carbon footprint.<sup>106</sup>

---

<sup>103</sup> <https://www.gamblingcommission.gov.uk/news/article/gambling-on-credit-cards-to-be-banned-from-april-2020#:~:text=UK%20Finance%20estimate%20that%20800%2C000,at%20some%20risk%20of%20harm.>

<sup>104</sup> The European Green Deal, section 2.1.1., Increasing the EU’s climate ambition for 2030 and 2050

<sup>105</sup> See for example [Tink](#), [Greenly](#), [Svalna](#) and other Fintechs

<sup>106</sup> See for example <https://wrap.org.uk/media-centre/press-releases/wasting-food-feeds-climate-change-food-waste-action-week-launches-help>

### 3.6.5.1 My Carbon Action

A Finnish FinTech, Enfuce,<sup>107</sup> has created My Carbon Action, a digital tool that allows banks and financial institutions to instantly calculate the carbon footprint of individual transactions. The calculation takes into account the environmental impacts of a product's entire lifecycle: from raw material extraction, manufacturing and transport, to use and disposal

The tool is based on a country-specific scientific data model, which ensures that the information is relevant in each use location. Additionally, My Carbon Action is based on users' own input regarding individual lifestyle choices. The lifestyle choices can relate to, for example, these main areas:

- Diet – are you vegan, lacto-ovo vegetarian or a meat-lover?
- Housing – do you live in a house or an apartment? How is it heated?
- Mode of transportation – walking, cycling, public transport, car sharing or your own car?
- Shopping – what is the origin of your purchase? How is it shipped and packaged?
- In the case of products bought, it is possible to calculate the environmental impact of a product's entire lifecycle from raw-material extraction, manufacturing and transport to use and disposal (not just buying), based on merchant category code, product level details, etc. The app, which is a B2B turnkey solution that banks and merchants can integrate into their existing app platforms, offers over a hundred personalised recommendations for greater sustainability.

Understanding the context and impact is extremely important. When banks can combine their transaction information with their customers' lifestyle choices, they can provide advice on more sustainable consumption. From the banks' point of view, they can use the My Carbon Action APIs flexibly to integrate them into their own apps and services – no new apps need to be built.

---

<sup>107</sup> <https://enfuce.com/>

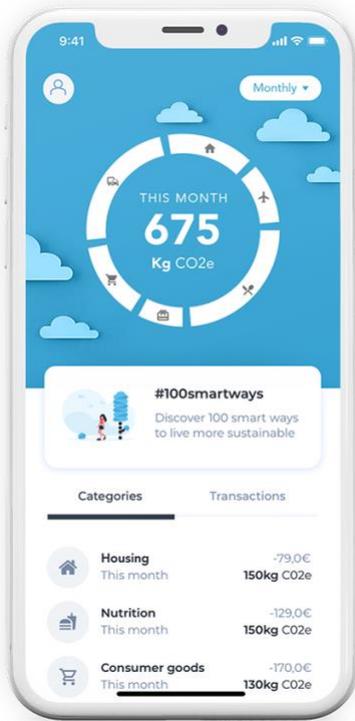


Figure 7: My Carbon Action in action

The country-specific data models and users’ own inputs make it possible to turn payment data into advice. The recommendations then help change behaviours and eventually governmental policy.

For banks, promoting more sustainable consumption is a way for a bank to manage its own risks, because in many situations ecological concerns tie in seamlessly with economic ones. By promoting better consumption amongst customers, banks are also indirectly reducing their own emissions.<sup>108</sup> It is a chance for the bank to showcase responsibility in concrete terms – by reducing emissions, instead of just reporting on financial activities. The best thing a bank can do is choose to see sustainability as an opportunity – instead of a cost or a burden. By addressing the customers’ sustainability concerns, a bank is responding not only to their current needs but also to those of the future – among the firsts.

### 3.6.5.2 Bank of the West

In July 2020, San Francisco-based Bank of the West launched a checking account in partnership with 1% for the Planet, that helps consumers to combat climate change.<sup>109</sup>

The account features a carbon-tracking tool from Doconomy<sup>110</sup> that details the carbon footprint of every purchase made and a biodegradable card.

In addition, one percent of net revenues generated from the account were donated to environmental non-profit organisations focused on creating a healthier planet. The first recipient of funds generated by the initiative was Protect Our Winters (POW).<sup>111</sup>

According to their CMO,

*“When you talk about climate change people are often at a loss as to what they can do personally to effect change. The 1% for the Planet Account allows consumers not only to bank with a group that is*

<sup>108</sup> As we have seen before, 70% of carbon emissions are driven by consumer behaviour. For example, handling money enables consumption, which means that banks are also enabling consumption-related emissions. Consumption-related emissions are therefore a joint effort between the banks and their customers

<sup>109</sup> [https://www.bankofthewest.com/about-us/press-center/press-releases/2020/2020-07-20-botw-launches-1percent-for-planet.html#:~:text=SAN%20FRANCISCO%2C%20CA%20\(July%202020,account%20designed%20for%20climate%20action.](https://www.bankofthewest.com/about-us/press-center/press-releases/2020/2020-07-20-botw-launches-1percent-for-planet.html#:~:text=SAN%20FRANCISCO%2C%20CA%20(July%202020,account%20designed%20for%20climate%20action.)

<sup>110</sup> <https://doconomy.com/>

<sup>111</sup> <https://protectourwinters.uk/>

*progressive on energy policy and is striving to meet the demands of the Paris Accord, but also that donates one percent of the account's revenue to address climate change at no cost to the consumer."*

### 3.6.5.3 Visa

In August 2020, Visa issued its first green bond offering, totalling 500 million USD, and appointed its first chief sustainability officer. The bond offering pays a semi-annual coupon of 0.75% and matures on 15 August 2027. The proceeds will be used to fund projects, including upgrades to buildings, energy efficiency improvements, expanded usage of renewable energy sources, water efficiency projects, employee commuter programmes, and research and initiatives focused on sustainable consumer behaviours.

### 3.6.5.4 Lloyds

In July 2021, Lloyds Banking Group announced a partnership with Ideavate, an energy-saving tech provider, whereby Ideavate's My Carbon Manager service is available to Lloyds Banking Group home insurance customers to help make their homes greener. Policyholders making a claim for a large leak or significant water damage where home renovations are needed, are given the option of accessing the My Carbon Manager app, which shows people how to make their lives more energy efficient. The tool is also available to Lloyds Bank and Bank of Scotland customers, and provides personalised suggestions and estimates on how to reduce their home's carbon footprint. Customers can use the app to see estimates for costs and savings and how carbon dioxide equivalent emissions could potentially be reduced. The tool is a one-stop guide on how policyholders can make their homes more environmentally friendly before looking for suppliers for repair work. All suggestions depend on the type of property and claim but could include options such as insulating walls or having solar panels fitted.

The app was created for the insurer by Ideavate, as part of a programme to support start-up insurtech companies. The service will be available for six months from July as part of a trial, with potential to be rolled out more widely for other types of large home insurance claims that need home renovation to be done, such as a large fire or flood.

## 3.6.6 Impact on Democracy

In July 2018, the UK's Nationwide Building Society selected seven FinTech companies to take part in its Open Banking for Good challenge, which launched in September 2018.<sup>112</sup> The FinTech firms committed to developing Open Banking based apps and services to help financially vulnerable people.

As the CEO of Nationwide said, "*While others may be looking at Open Banking through a commercial lens, Open Banking for Good is driven by our social purpose.*"<sup>113</sup>

The seven companies selected were chosen from more than 50 applicants and fall into three categories:

- **Income and Expenditure:** Openwrks and Ducit.ai

<sup>112</sup> <https://www.bristol.ac.uk/media-library/sites/geography/pfrc/2019-12-moving-the-dial.pdf>

<sup>113</sup> <https://www.nationwidemediacentre.co.uk/news/seven-fintech-firms-join-forces-with-nationwide-to-address-financial-capability-issues>

- **Income Smoothing:** Trezeo and Flow
- **Money Management and Help:** Toucan, Squad and Tully

The challenge, born of the Inclusive Economy Partnership, was supported by a 3 million GBP fund from Nationwide. The start-ups are also able to draw on expertise from Nationwide, Money Advice Trust, Citizens Advice, The Money Charity, Money and Mental Health Policy Institute, Accenture, Doteveryone and Nesta.

A big sub-topic of Open Banking for Good generally is to create a movement to use Open Banking, not just for making money, but making the world better by using a mix of financial and other data to improve CO<sup>2</sup> reduction (by tracking travel, steak house visits etc), equal pay, gender discrimination, financial inclusion.

### 3.6.6.1 Financial Inclusion

The past 20 years have seen strong growth in self-employment in the UK, which now has more than five million self-employed people who represent around 15% of the workforce, up from 12% in 2000.<sup>114</sup> In addition, nearly one in 10 workers do platform work at least once a week (i.e. jobs found via a website or app like Uber, Deliveroo or Handy).<sup>115</sup> While individuals may value the flexibility offered by these types of work, research shows that irregular income patterns and related economic security issues represent the biggest challenges these workers face.<sup>116</sup> Providing individuals with Open Banking-based tools to vastly improve their money management and cash-flow issues helps to reduce fatigue and mental anxiety.

## 3.6.7 Contributions to the EU CyberSecurity Strategy for the Digital Decade

Further research into Open Banking cybersecurity will make an important contribution to the success of the EU Cybersecurity Strategy for the Digital Decade.<sup>117</sup>

### 3.6.7.1 Resilient infrastructure and critical services

The European Cybersecurity Strategy highlights the critical importance of increasing the level of “*cyber resilience of all relevant sectors, public and private that perform an important function for the economy and society.*” From this it can be inferred that financial institutions are expected to “*strengthen digital operational resilience and ensure an ability to withstand all types of ICT-related disruptions and threats.*” Referencing the revised NIS Directive (NIS2):<sup>118</sup>

*The financial sector must also strengthen digital operational resilience and ensure an ability to withstand all types of ICT-related disruptions and threats, as the Commission has proposed.*<sup>119</sup>

Similarly, NIS2 itself identifies financial services as one of the seven sectors essential for ensuring the resilience of digital infrastructure and other critical services in Europe.

---

<sup>114</sup> ONS, 2020

<sup>115</sup> TUC, 2019

<sup>116</sup> Lockey, 2018

<sup>117</sup> <https://ec.europa.eu/digital-single-market/en/cybersecurity-strategy>

<sup>118</sup> European Commission, Directive on measures for high common level of cybersecurity across the Union (revised NIS Directive or “NIS 2”), COM(2020) 823

<sup>119</sup> Here referring to [DORA, the proposal for a regulation on digital operational resilience for the financial sector](#)

To that end, the growing adoption of Open Banking, not only in Europe but worldwide, will attract increased attention from malevolent actors and accelerate the urgency to address the security issues reported here. In addition, the work being carried out in the demonstrator use cases, notably the creation of a “fighting fraud network” as well as the use of safe, verifiable credentials for authentication purposes, have a significant role to play in addressing the concerns outlined in the European Cybersecurity Strategy.

The financial sector is greatly dependent on information and communication technologies (ICT). The importance of ensuring remote access to financial services increased to an even greater extent during the COVID-19 pandemic, with a 72% increase in the use of financial applications in Europe.<sup>120</sup> This reliance on ICT has triggered, since the beginning of the pandemic, a 38% increase in cyberattacks on financial institutions,<sup>121</sup> which national regulators, otherwise occupied, have struggled to effectively address. This was one of the motivations for the adoption on 24 September 2020 of DORA (a proposal for a regulation that requires institutions in the financial industry to improve their cybersecurity), accompanied by a directive<sup>122</sup> that includes a digital finance strategy and legislative proposals on crypto-assets and digital resilience.<sup>123</sup>

Perhaps not surprisingly, there were duplicate rules set out in NIS2, which is tasked with amendments to financial services directives to introduce cross-references to the DORA and to update empowerments for technical standards.

In order to achieve its objectives, the European Commission is extending the applicability of the rules to 20 types of regulated EU financial entities, such as banks, stock exchanges and clearinghouses, as well as FinTechs.

Information sharing allows financial entities to set up arrangements to exchange among themselves cyber threat information and intelligence on tactics, techniques, procedures, alerts and configuration tools in a trusted environment.<sup>124</sup> Information sharing in fighting fraud and eKYC plays a key role in the research being carried out in CyberSec4Europe which is where the project can make a considerable impact.

Although the DORA is still only a proposal, it should be a much welcomed catalyst in efforts to build the digital single market for financial services comprehensive framework at the EU level, setting out rules on digital operational resilience for all regulated financial entities, which would address ICT risks more comprehensively, enable financial supervisors’ access to information on ICT-related incidents, ensure that financial entities assess and identify ICT vulnerabilities, strengthen the outsourcing rules governing the indirect oversight of ICT third-party providers, enable direct oversight of the activities of ICT third-party

---

<sup>120</sup> The European Commission: Digital Finance Factsheet (2020)

<sup>121</sup> *ibid*

<sup>122</sup> The European Commission: Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341. COM/2020/596 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0596>.

<sup>123</sup> [The European Commission: Digital finance package \(2020\)](#).

<sup>124</sup> See Article 40 and Explanatory Memorandum of the DORA

providers when they provide their services to financial entities, and additionally, incentivise the exchange of threat intelligence in the financial sector.<sup>125</sup>

### **3.6.7.2 Building a European Cyber Shield**

This vertical does not directly contribute to this dimension.

### **3.6.7.3 An ultra-secure communication infrastructure**

This vertical does not directly contribute to this dimension.

### **3.6.7.4 Securing the next generation of broadband mobile networks**

This vertical does not directly contribute to this dimension.

### **3.6.7.5 An Internet of Secure Things**

This vertical does not directly contribute to this dimension.

### **3.6.7.6 Greater global Internet security**

As mentioned above, the security and resilience of the European financial sector are inextricably bound up with activities globally and it is vital that there is a multi-party sharing of cybersecurity threat information, as well as latest research and development results.

### **3.6.7.7 A reinforced presence in the technology supply chain**

This vertical does not directly contribute to this dimension.

### **3.6.7.8 A Cyber-skilled EU workforce**

This vertical does not directly contribute to this dimension.

### **3.6.7.9 EU leadership on standards, norms and frameworks in cyberspace**

The EU is a respected leader internationally in the development and implementation of new standards and frameworks, and this includes those areas pertaining to Open Banking. However, as noted above, even though Europe has made great strides in framing new legislation and implementing new developments, banking in the US and payments in Asia are moving ahead at pace, and it is important for Europe to increase the adoption of secure Open Banking in all sectors of financial services and to demonstrate the benefits and security aspects of new applications.

### **3.6.7.10 Cooperation with partners and the multi-stakeholder community**

It should almost go without saying that the strength and viability of all the effort that has gone into the development and framing of secure Open Banking will be squandered without active and robust cooperation

---

<sup>125</sup> The European Commission: COMMISSION STAFF WORKING DOCUMENT EXECUTIVE SUMMARY OF THE IMPACT ASSESSMENT Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014. SWD/2020/199 final.

in a multi-stakeholder community – meaning not just banks, merchants, payments companies and FinTechs, but also from dependent parties across multiple vertical sectors.

### 3.6.7.11 Strengthening global capacities to increase global resilience

Europe’s aspiration to being a leader in Open Banking standards, services and security implies taking a strong collaborative role at a global level. To draw a parallel with the pandemic, capacity and resilience in any one socioeconomic geographic domain is highly dependent on all the others: i.e. the global financial community has to work together!

## 3.6.8 Brexit Dimension

Brexit clearing warrants a discussion of its own. On the positive side, this will allow the UK to forge ahead, also in Open Banking, unfettered by some of the more curious regulations that have been imposed by Brussels. Some regulations around APIs (not tight enough) and authentication (too tight) can then be defined within the UK in a better way.

However, the main impact will be negative.

- Firstly, and practically, all the eIDAS certificates (one of the fundamental identifying mechanisms that are the basis of identifying the parties) had to be revoked and replaced with a national solution. In July 2020, the EBA announced that eIDAS certificates of UK TTPs would be revoked when the Brexit transition period ended on 31 December 2020. eIDAS certificates are required for TTPs to identify themselves to AISPs and allow firms to interact and share customer account information online in a trusted and secure way. Under the SCA-RTS, eIDAS certificates are the only accepted identification standard permitted between providers of Open Banking services in the EU. Hence, in November 2020, the UK’s FCA (Financial Conduct Authority) announced changes to Open Banking identification requirements to limit the risk of disruption to Open Banking services after 2020. The changes will permit UK-based TTPs to use an alternative to eIDAS certificates to access customer account information from account providers, or initiate payments.

As companies are expected to ensure that they can continue to provide Open Banking services, these changes mean:

- UK-based TTPs have to obtain a new certificate to be able to continue to provide Open Banking services in a post-Brexit UK;
- AISPs and PISPs (e.g. banks) have had to make technical changes to their systems to enable TTPs to continue accessing customer account information, by accepting an alternative certificate and informing TTPs as soon as possible which certificate(s) they will accept;

In an acknowledgement of the challenges faced by the industry, the FCA provided a transition period until the end of June 2021 for UK banks and others to comply with the rules.

- Secondly, the passporting of FinTechs that gained a licence in one Member State and can therefore operate smoothly in the rest of the Member States ceased. Those who had a Revolut account already

felt the major consequences of this personally (many emails sent to all customers about how the UK banking licence is being transferred to Lithuania, with IBANs<sup>126</sup> changing etc.).

There is also some concern (depending on how treaties may be drawn up) about joint security cyber defence between nations. Not much can be done about all this from a CyberSec4Europe point of view, except maybe to devise mechanisms to mitigate some of the most egregious separation effects.

### 3.6.9 Sector-specific Dimensions

#### 3.6.9.1 The United States

Although Germany introduced FinTS / HBCI<sup>127</sup> over 20 years ago, many consider that the United States is where Open Banking really began: American FinTechs have been building applications for decades that allowed financial institutions to connect multiple accounts on behalf of their customers, without having any regulations in place. In Europe, these applications only started to be developed when PSD2 came into force. In essence, the US is ahead in market penetration, but Europe is ahead in regulation.

But the US will eventually catch up. On 9 July 2021, President Biden issued an ‘Executive Order on Promoting Competition in the American Economy’<sup>128</sup> with significant consequences for the banking sector – more data sharing.

Amongst 72 initiatives, the Executive Order:

- Aims to “Make it easier and cheaper to switch banks by requiring banks to allow customers to take their financial transaction data with them to a competitor.”
- “Encourages the Consumer Financial Protection Bureau (CFPB) to issue rules allowing customers to download their banking data and take it with them.”

According to Politico,<sup>129</sup> the order is expected to support open banking regulations, which seek to allow data sharing among financial firms to increase consumer convenience and price transparency. New regulations could provide more clarity about the consumer protection and cybersecurity obligations of financial apps that have access to data from customers’ bank and brokerage accounts.

Under the 2010 Dodd-Frank law,<sup>130</sup> consumers have the right to access their own financial data, although the CFPB has yet to issue standards that would govern consumer requests and transfers.

It is well-known that the US is market-driven and normally does not like governments telling industry what to do, but it appears that the Biden administration is frustrated at the lack of innovation from banks.

---

<sup>126</sup> IBAN: International Bank Account Number

<sup>127</sup> FinTS (Financial Transaction Services), formerly known as HBCI, is a bank-independent protocol for online banking, developed and used by German banks. HBCI was originally designed by the two German banking groups Sparkasse and Volksbanken und Raiffeisenbanken and German higher-level associations as the Association of German Banks.

<sup>128</sup> <https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/09/fact-sheet-executive-order-on-promoting-competition-in-the-american-economy/>

<sup>129</sup> <https://www.politico.com/news/2021/07/08/biden-assault-monopolies-498876>

<sup>130</sup> <https://www.congress.gov/111/plaws/publ203/PLAW-111publ203.pdf>

It remains to be seen how effective this wide-ranging order will be and how long it will take, but, as a statement of intent, the direction is clear.

Previously, in August 2019, the US Department of the Treasury published a report<sup>131</sup> aimed at promoting innovation in the areas of loans, payments and wealth management, which also sets the limits for managing open banking. The report recognised the need to remove legal and regulatory uncertainties that currently prevent financial services companies and data aggregators from establishing data-sharing agreements but did not envisage an Open Banking model along the lines of the UK's as the solution.<sup>132</sup>

The recommendation highlights were twofold: that:

- The Bureau of Consumer Financial Protection (CFPB) should affirm that Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (which states that financial services companies subject to the Bureau's jurisdiction are required to make available to a consumer, upon request, certain financial account and transaction data) also applies to third parties authorised by consumers, including data aggregators and FinTech application providers.
- The US market would be best served by a solution developed by the private sector, with appropriate involvement of federal and state financial regulators.

Prior to this report the CFPB had published non-binding Consumer Protection Principles<sup>133</sup> aimed at consumer-authorized financial data sharing and aggregation and advocating giving consumers access to their own data in a useable format, as well as allowing them to authorise read-only third-party access, informed consumer consent, data security and dispute resolution.

To date, although API standards have been neither established nor agreed in the US, FinTechs have resorted to accessing consumer data by "screen-scraping". Although the Treasury Department does not require banks to open up through APIs, it does recommend that regulators remove the legal and regulatory uncertainties that are

*"preventing financial services companies and data aggregators from entering into agreements to migrate from screen scraping to more secure and efficient API-based data-sharing methodologies."*

However, some banks are developing their own open APIs, and NACHA, the National Automated Clearinghouse Association for electronic payments, created the API Standardization Industry Group, which has identified specific APIs for development, including some on data sharing.

The reluctance of US financial institutions to open up to FinTechs is due in large part to the absence of security and regulatory safeguards. Despite its many benefits, Open Banking does engender financial risk. To that end, the US Treasury Department recommends that banking regulators eliminate the ambiguity that

<sup>131</sup> A Financial System That Creates Economic Opportunities Nonbank Financials, FinTech, and Innovation, <https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf>

<sup>132</sup> Ibid: "[t]here are significant differences between the United States and the United Kingdom with respect to the size, nature and diversity of the financial services sector and regulatory mandates."

<sup>133</sup> [https://files.consumerfinance.gov/f/documents/cfpb\\_consumer-protection-principles\\_data-aggregation.pdf](https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf)

discourages banks from adopting more secure data access methods, such as APIs, which may provide the incentive to compete.

In response to the Treasury report's recommendation, the CFPB has indicated that it will issue advance notice of proposed rulemaking on Open Banking in the United States by the end of 2020 that will seek to implement section 1033 of the Dodd-Frank Act. This will determine how consumers' access to their financial information is regulated<sup>134</sup>, a future decision on which could put the US on a path to a more standardised Open Banking system, similar to that in Europe.

Until now, consumer access to financial data sharing in the US has been largely dependent on private-sector efforts. For example, the Financial Data Exchange (FDX) is a financial industry consortium, with over 100 members, that has promoted its own data-sharing principles<sup>135</sup>. However, going forward the US requires a governmental body to issue guidance on how financial institutions – particularly major banks – handle financial data sharing, which would carry the weight of a regulatory obligation to comply. This standardised approach to Open Banking would be a boon for FinTechs and, through improved customer experiences, a boost for banks too.

The US may be late in aligning the necessary steps to establish a workable approach to open banking, but it is reasonable to expect that the results will be tangible within the coming one to two years.

### 3.6.9.2 Asia

In Europe the focus is still very much on cards<sup>136</sup> - a technology of 30 years' standing. It has been serving us well, but the time has come to think of more modern alternatives. Even virtual cards (where the reliance is no longer on the physical piece of plastic, but still employs the old rails with 16-digit card numbers) cannot be the answer. In Asia, by contrast, there is a huge focus on the mobile phone, specifically an explosion of apps that provide not only payment, but a complete solution for many life situations. Most famous is AliPay by Ant Financial, who has become the lifestyle companion of choice.

AliPay allows you to spend money in a shop, but also to take out loans, find where your friends are shopping, get recommendations where to get special offers based on your preferences, how to save for retirement etc.

---

<sup>134</sup> [Consumer Access to Financial Records](#): *Section 1033 of the Dodd-Frank Act provides, among other things, that subject to rules prescribed by the CFPB, a consumer financial services provider must make available to a consumer information in the control or possession of the provider concerning the consumer financial product or service that the consumer obtained from the provider. The CFPB is issuing this Advance Notice of Proposed Rulemaking (ANPR) to solicit comments and information to assist the Bureau in developing regulations to implement section 1033.*

<sup>135</sup> [Financial Data Exchange Refines Vision for Consumer-First Financial Data Sharing Practices](#)

<sup>136</sup> See repeated ECB calls that we need a European payment *card* to improve sovereignty vs the American schemes Visa/Mastercard/AmEx/PayPal e.g. <https://www.ecb.europa.eu/press/pr/date/2020/html/ecb.pr200702~214c52c76b.en.html> and the industry response EPI (European Payment Initiative) which is setting up a pan-European *card* scheme and wallet

This combination of financial services and connecting you to your friends and favourite retailers is often called ‘social commerce’.

These all-encompassing apps (not just a payment button or a card as in Europe) are used all the time by hundreds of millions of people in many Asian countries. AliPay has over a billion daily active users<sup>137</sup>. When Chinese tourists land in Frankfurt, the first thing they do is open up AliPay to see how to get to their hotel, to navigate to a duty-free shop at the airport with staff who speak Chinese and where one can use AliPay as payment, get messages from their friends, get offers for a bus tour around the old town, etc. They never need to leave AliPay.

This model is conquering Asia, for example:

- WeChat (China)
- Line (Japan)
- Grab (Singapore)
- Go-Jek (Indonesia)
- Paytm (India)

Payment at a physical shop in Asia is often triggered by a QR code. The customer holds his phone to the merchant’s QR code and AliPay will ask for confirmation and the money is settled. QR codes have been very successful as they require little infrastructure/investment at the merchant (in its simplest form just a static QR code sticker at the checkout) and is possible on every phone that has a camera. No large requirements for IT on either side.

European banks have sometimes misunderstood the AliPay success to be due to QR codes and have tried to add a QR feature to their bank and card apps. But just adding a QR code alone does not make a great difference – the key is in the social commerce and getting everything integrated in one lifestyle app.

In Europe we also, for some reason, put this focus on the young (who have little money). In Asia these apps are targeted at everyone: the businessman, the middle aged (both of whom do have money), the rural population – all. That is why it is pervasive and hence also the method of choice for exchanging money (P2P via app<sup>138</sup>).

These super apps, that do much more than just the one thing, are conquering Asia with millions of users each. Some of these super apps have grown from messaging (AliPay), some from ride-sharing (GoJek),

---

<sup>137</sup> See sample statistics under <https://www.chinainternetwatch.com/tag/alipay/#:~:text=Alipay%20is%20China's%20leading%20online,the%20course%20of%20a%20year>.

<sup>138</sup> At Chinese festivals, the little red envelopes with money are increasingly being replaced by digital money sending. Already in 2016, over the six-day Chinese Spring Festival, 516 million people sent and received 32 billion digital red envelopes – ten times the number over the same period the year before (See <https://www.bbc.com/news/business-38746298>). It is also an extraordinary success for P2P (peer-to-peer/person-to-person) sending money.

some from ordering takeout, some from social media, some from banking: in the end they all converge on all services.

Their goals are to captivate loyalty and engagement and provide convenience and seamlessness above all. As the app adds new services, its usefulness causes it to become more intertwined in consumers' daily lives. Some say these apps are on their way to becoming 'super brands'. Consumers' trust and loyalty increase as the super app consolidates more and more services ultimately stealing share from other companies. Having gathered more and more data from their users, these data-rich businesses see an opportunity to offer better financial services to a massive pool of users who they understand better than anyone else. In doing so they further extend their ownership of the user experience. A virtuous circle <sup>139</sup>.

Sidu Ponnappa, SVP of engineering at GOJEK, stressed the importance of payments in super apps: "The biggest moat GOJEK built is payments. Once you're handling money for a user, you can build a castle of services within it." <sup>140</sup> Which is rather a different story to introducing a new plastic card in Europe!

### 3.6.10 Summary of the dimensions and impact on the roadmap

The previous sections give an overview of the different dimensions and how they interact with Open Banking.

As is apparent, the pace of development and implementation of Open Banking applications and innovation is growing rapidly worldwide, although there is considerable scope for further adoption. The concerns that exist around privacy and security, and in particular the conflicting requirements of the GDPR and PSD2 in Europe, are still prevalent. What is interesting is the influence of open banking, which may impact, or may have already impacted dimensions not directly related to the financial community. As with many other sectors, it is also clear with Open Banking that global cooperation is vital to ensure resilience and seamless, secure interoperability, both in Europe and globally. Although Europe has demonstrated real leadership in developing Open Banking concepts, alongside the revised PSD, the rest of the world is catching up and, in some cases, diverging from a common model.

### 3.6.11 Challenge 1: Mapping of stakeholder interaction in end-to-end Open Banking processing

Despite the need for an end-to-end view over all actors, it is believed that no-one has yet mapped the whole Open Banking process end-to-end. It would be a very worthwhile exercise to draw a map of all the stakeholders involved, how they interact, how they rely on each other and how the chain of trust is built. It is to be expected that a number of gaps will become apparent. These gaps in security and privacy must be identified and closed.

#### Specific research goals

- **End-to-end processing.** Identifying and closing the gaps in security and privacy in the Open Banking process

---

<sup>139</sup> Although some, even the Chinese government, are becoming increasingly wary of the dominance of these platforms

<sup>140</sup> Source: <https://www.linkedin.com/pulse/what-super-app-sidu-ponnappa?articleId=6570584548118228993>

### JRC Cybersecurity Domain: Data Security and Privacy

- Privacy requirements for data management systems;
- Design, implementation, and operation of data management systems that include security and privacy functions;
- Privacy by design and Privacy Enhancing Technologies (PET)

### JRC Cybersecurity Domain: Security Management and Governance

- Compliance with information security and privacy policies, procedures, and regulations

### JRC Sectorial Domain: Financial

- Banking services

#### 3.6.12 Challenge 2: Setting up and discontinuing business relationships

For this not only the “steady state” will need to be examined, but also the setting up and discontinuation of any relationships.

- How does a national authority inform central authorities, and then banks rely on this information, as a FinTech sets up business?
- What happens if there is a breach or a fraud and how does the system protect the perimeter?
- What happens if a consent or licence needs to be suspended or withdrawn – how are the relevant parties informed in a timely, secure manner?

#### Specific research goals

- *Severing relationships.* To answer the questions outlined above – and other similar challenges – will require systematic security analysis, modelling and implementation of solutions using modern methods that go beyond what is specified in the various pieces of legislation.

### JRC Cybersecurity Domain: Data Security and Privacy

- Privacy requirements for data management systems;
- Design, implementation, and operation of data management systems that include security and privacy functions;
- Privacy by design and Privacy Enhancing Technologies (PET);

### JRC Cybersecurity Domain: Security Management and Governance

- Compliance with information security and privacy policies, procedures, and regulations;

### JRC Sectorial Domain: Financial

- Banking services

#### 3.6.13 Challenge 3: Cross-border cooperation under differing legislation and security controls

The need for many stakeholders to work together and ensure an unbroken chain of trust, which will occur within any Member State, will be further exacerbated when stakeholders are distributed across borders.

- **Legislation:** Different national competent authorities have differing licensing regimes<sup>141</sup> and different courts have different interpretations of legislation, primarily, but not exclusively, associated with PSD2.
- **Protocols and APIs:** Italy's RI.BA<sup>142</sup> and Bolletino payment schemes use different protocols to those of iDeal<sup>143</sup> in The Netherlands and different banks offer different APIs which could be based on the those proposed by, for example:
  - **The Open Banking Implementation Entity (OBIE)**<sup>144</sup> is a company set up by the CMA in 2016 to deliver Open Banking, primarily for, but not limited to, the UK market.
  - **The Berlin Group**<sup>145</sup> is a pan-European payments interoperability standards and harmonisation initiative with the primary objective of defining open and common scheme- and processor-independent standards in the interbanking domain between a creditor bank (acquirer) and a debtor bank (issuer), complementing the work carried out by, for example, the European Payments Council (EPC). As such, the Berlin Group was established as a pure technical standardisation body, focusing on detailed technical and organisational requirements to achieve this primary objective. The Berlin Group consists of almost forty banks, associations and PSPs from across Europe.
  - **STET**, the payment processor owned by France's six major banks, developed a standardised open-access API and companion testing platform to enable banks and FinTechs to meet regulatory and legal requirements, ensure smooth integration between apps and bank infrastructure and expedite time to market for new services.
  - And others
- **Security:** the implementation of security measures varies considerably: for example, online banking is authenticated very differently in the UK and in Germany.

### Specific research goals

- **Harmonisation of national legislation.** In order to maintain any semblance of cross-border interoperability in and across Europe, the diversity of licensing regimes and legislative interpretations, have to brought under a pan-European umbrella that provides a working model that ideally can be developed to scale worldwide.
- **Harmonisation of protocols and APIs.** In order to maintain any semblance of cross-border interoperability in and across Europe, the diversity of protocols and APIs have to brought under a pan-European umbrella that provides a working model that ideally can be developed to scale worldwide.

<sup>141</sup> As PSD2 is a directive, it means that there are 27 national translations of the law

<sup>142</sup> The most common instrument for business-to-business (B2B) collections is the [Ricevuta Bancaria](#) (RI.BA or Riba) while business-to-consumer (B2C) collections (e.g. for insurance premiums or utility bills) are usually performed via the Italian direct debit, [Rapporto Interbancario Diretto \(RID\)](#)

<sup>143</sup> [iDEAL](#) is an online payment method based on a four-corner model which generates a SEPA Credit Transfer from within the consumers trusted online banking portal. By using iDEAL consumers are able to pay for their online purchases in a user-friendly, cost-efficient and secure fashion. Merchants receive real-time confirmations of the iDEAL payments which are guaranteed and irrevocable.

<sup>144</sup> <https://www.openbanking.org.uk/>

<sup>145</sup> <https://www.berlin-group.org/>

- **Harmonisation of security controls.** In order to maintain any semblance of cross-border interoperability in and across Europe, the diversity of security measures have to be brought under a pan-European umbrella that provides a working model that ideally can be developed to scale worldwide.

#### JRC Cybersecurity Domain: Data Security and Privacy

- Privacy requirements for data management systems;
- Design, implementation, and operation of data management systems that include security and privacy functions;
- Privacy by design and Privacy Enhancing Technologies (PET)

#### JRC Cybersecurity Domain: Security Management and Governance

- Compliance with information security and privacy policies, procedures, and regulations;

#### JRC Sectorial Domain: Financial

- Banking services

### 3.6.14 Challenge 4: Convenient and Compliant Authentication

Open Banking and the new innovative FinTech ecosystem will only succeed and provide the benefits of innovation, transparency, cost reduction and competition if users can use the new services easily. On the other hand, it is imperative to verify explicit user consent, to adhere to the complex secure customer authentication rules, to embed any solution in existing online and mobile banking and mobile and e-commerce practices.

#### Specific research goals

- **Improving the user experience.** To resolve the constraints associated with making Open Banking easy to use, consent-based and secure, work has to be undertaken to disambiguate the apparent conundrum that Open Banking has with needing to enforce compliance with the GDPR and implementing PSD2. In other words, assuring users that the banks and financial institutions are at the very least as secure as they were considered to be in the past alongside being transparent about the openness and access now afforded by the banks to FinTechs.

#### JRC Cybersecurity Domain: Data Security and Privacy

- Privacy requirements for data management systems;
- Design, implementation, and operation of data management systems that include security and privacy functions;
- Pseudonymity;
- Unlinkability;
- Privacy by design and Privacy Enhancing Technologies (PET);
- Data usage control

#### JRC Cybersecurity Domain: Human Aspects

- Usability
- User acceptance of security policies and technologies
- Individual, organizational, and group information privacy concerns and behaviours;
- Privacy attitudes and practices

#### JRC Cybersecurity Domain: Identity and Access Management (IAM)

- Authentication/Access Control Technologies (X509 certificates, RFIDs, biometrics, PKI smart cards, SRAM PUF etc.)

#### JRC Sectorial Domain: Financial

- Banking services

### 3.6.15 Challenge 5: Real time Revocation of Right of Access

The regulations speak a great deal about how to set up the relevant consent processes, licensing processes, how to get certificates from which authorities, etc. One area that is very underserved, however, is the area of *revocation* of consent, *withdrawal* of licence, *suspension* of access pending dispute resolution. Indeed, the regulatory texts contain some quite frightening passages in this context: for example, that one regulator passes the information on to the next “within 24 hours” or “as soon as possible” or “within a few working days”. If a merchant, or TPP/FinTech, or customer or indeed bank should turn rogue at any time (reselling data, initiating fraudulent payment, etc.), it is essential to stop access immediately (including at weekends and national holidays!) and in real time and across the whole ecosystem for that bad actor.

#### Specific research goals

- **Real time revocation of right of access.** Given some of the ambiguities in the regulatory language pertaining to the rescinding of access rights in the case of bad actors, particularly with respect to the timing of notification, it is critically important to provide clarity and the cross-border infrastructure to carry out the analysis, detection, communication and real time action without damaging innocent others or causing systemic problems.

#### JRC Cybersecurity Domain: Operational Incident Handling and Digital Forensics

- Incident analysis & Documentation;
- Containment Strategy design;
- Incident response;
- Vulnerability analysis & response

#### JRC Cybersecurity Domain: Security Management and Governance

- Continuous monitoring;
- Compliance with information security and privacy policies, procedures, and regulations;
- Incident management and disaster recovery;
- Reporting (e.g. disaster recovery and business continuity)

#### JRC Sectorial Domain: Financial

- Banking services

### 3.6.16 Challenge 6: Corporate Open Banking Security

It was observed above that the most commercial activity in Open Banking may actually be in the B2B space. Many FinTechs are developing solutions explicitly for corporate use, not for consumers. The regulator has explicitly permitted this and exempted corporate users from many of the secure customer authentication measures to allow the continued use of existing corporate authentication practices. These – in contrast to consumer authentication – are typically, but not exclusively, a reliance on:

- *multi*-authentication: for example, the treasurer and the head of personnel may *both* need to release the salary payments of a company;

- *roles*, defining which individuals may sign off for a certain value of payments in specified contexts;
- *different authentication technologies*, such as iris recognition in military-grade contexts, enhanced use of chip cards to identify roles etc.

### Specific research goals

- **Mitigation of corporate risks.** Although the focus of security concerns relating to Open Banking are in relation to B2C, by far the biggest value payments are exchanged in B2B. As a consequence, the exposure of corporates to the risk of unregulated and/or non-standard secure procedures and processes could be considered an oversight that should be remedied by a thorough examination of the specifics of corporate open banking and specifically corporate authentication practices to see which risks are involved and how to mitigate them.

### JRC Cybersecurity Domain: Data Security and Privacy

- Privacy requirements for data management systems;
- Design, implementation, and operation of data management systems that include security and privacy functions;
- Data usage control

### JRC Cybersecurity Domain: Security Management and Governance

- Privacy Risk management

### JRC Sectorial Domain: Financial

- Banking services

## 3.7 Mapping of the Challenges to the Big Picture

### Challenge 1: Mapping of stakeholder interaction in end-to-end Open Banking processing

The introduction of AISPs and PISPs in Open Banking has been completely disruptive to traditional banking processes for payments, the security of which had evolved over decades if not longer. It comes as little surprise then that, with the introduction of new actors in the transaction chain from customer to financial institution, there are some aspects of possible scenarios and interactions in the new end-to-end process for financial transactions that are not covered by PSD2.

### Challenge 2: Setting up and discontinuing business relationships

The continuing theme in our security-focused approach to Open Banking is that the wholesale changes to third party access to banks have disrupted well-established and proven practices. For example, with the insertion of potentially new third parties including FinTechs into the payment process, the old mechanisms for establishing and severing relationships are not always valid and present a back door for corporate malfeasance.

### Challenge 3: Cross-border cooperation under differing legislation and security controls

As PSD2 is ‘only’ a directive, Member States and Associated Countries are able to interpret aspects of the legislation differently – and do, either through state institutions or appointed industry bodies. Notable is the discrepancy in the approach to APIs across Europe – and globally – which is in dire need of resolution.

#### Challenge 4: **Convenient and compliant authentication**

Users are now having to engage with new and unfamiliar mechanisms for processing payments and allowing access to their banking assets. With the uncertainty engendered by Open Banking and its concomitant concepts – for example, the provision of consent to third parties to get direct access to users’ bank accounts – there are genuine user concerns about the security of any apparent changes in mechanisms for authentication or consent requests.

#### Challenge 5: **Real time revocation of right of access**

A benefit of PSD2 – being able to pass on the right of access – is also a potential loophole, if users are careless or duped into providing access to rogue actors; or simply if a bank’s customer wishes, for one of any number of reasons, to terminate an access right previously awarded. This is a ‘new’ problem and one that has to be addressed in real time which it isn’t at present.

#### Challenge 6: **Corporate open banking security**

Similar to Challenge 1, not all aspects of the new end-to-end process for B2B financial transactions are covered by PSD2. Nor have they received the same degree of attention as B2C transactions, even though Open Banking has as much potential – if not more. Needless to say, the potential damage associated with any security breach is also considerably greater, hence the urgency to investigate areas that are not adequately protected.

### **3.8 Methods, Mechanisms, and Tools**

This section presents the mechanisms and tools needed to address the challenges described above. It also indicates which of these are being developed in WP3 and what additional methods need to be developed. Table 2 summarises the challenges identified in the Open Banking vertical and the tools needed to address them

#### **3.8.1 Challenge 1: Mapping of stakeholder interaction in end-to-end Open Banking processing**

*Method:* Until recently banks and other financial institutions had established mechanisms and processes for securely processing end-to-end transactions. To date, having direct peer-to-peer relationships with their customers, it was relatively straightforward for banks to put in place one or two factor authentication mechanisms that could be regularly enhanced, particularly on the back of the requirements of a physical KYC discipline as a key component of the onboarding procedure.

Consequently, the introduction of AISPs and PISPs is disruptive, as not all aspects of the new processing of financial transactions are covered by PSD2 and potential privacy issues that would impact GDPR compliance may be exposed.

In order to identify the gaps in security and privacy, the initial approach is to map the processes end-to-end, taking into account both internal and external systems, involving all stakeholders in B2C banking and payment transactions including users. Once this task is undertaken, the gaps identified can be addressed and closed.

*Mechanism:* After a small number of financial institutions which are prepared to cooperate are engaged, the first step is to pick a small set of processes that are representative of a range of transactions of varying degrees of complexity that traverse the whole eco-system including multiple actors. For the movement of data across the entire transaction chain, the primary potential weak points are likely to be SSL authentication, XML and endpoint security.

*Tools:* For this initial stage, general-purpose methodologies such as OFMC/AIF and CORAS, (both D3.1, Section 5.2), could be used to assess the system vulnerabilities, whereas subsequent actions could benefit from tools such as DP analysers and Security & Privacy by Design (both D3.1, Section 5.1).

### **3.8.2 Challenge 2: Setting up and discontinuing business relationships**

*Method:* The insertion of new third parties, including FinTechs, into Open Banking payment processes has disrupted the old mechanisms for establishing and severing relationships between financial institutions and their customers. As in many cases the tried and tested arrangements are no longer valid, although some will be covered by existing legislation. Although in many scenarios the lack of adequate provision will not be an issue, in the case of disruption, a systematic security analysis followed by the modelling and implementation of solutions are required to cover the scenarios that are not otherwise covered.

*Mechanism:* The failing is not being able to ensure the trustworthiness of all the third parties that enter into a transaction process. A disruptive scenario that could adversely impact the integrity of a banking/financial ecosystem could arise as a result of a fraudulent or negligent third party acting on behalf of a customer. At the point the third party in question is either uncovered, ‘disappears’ or goes out of business, if there is no legal redress, the ensuing circumstances that could impact all the other actors in the process chain could be catastrophic.

The mechanism to be adopted is first to identify the scenarios that are covered by existing legislation. As a result of the analysis, the next stage would be to implement solutions to be communicated to the relevant national and supranational authorities.

*Tools:* Once the untrustworthy scenarios have been identified, a tool such as Trust Monitor (D3.1, Section 5.1) could be used to monitor suspicious or unusual behaviour by third parties.

### **3.8.3 Challenge 3: Cross-border cooperation under differing legislation and security controls**

*Method:* As PSD2 is ‘only’ a directive, Member States and Associated Countries are at liberty to interpret aspects of the legislation differently. Notable is the lack of an implementation entity for the EU and in particular the discrepancy in the approach to APIs: there is no cross-bank or pan-European API standards have yet to be clarified. Creating these standards is vital: If PSD2 is to develop a unified, innovative, pan-European digital ecosystem for financial products, and uniform interfaces and processes, standards are essential for achieving this goal.

There are three different approaches to tackling this disconnect that are primarily in the realm of policy recommendations.

*Mechanism:*

- To achieve a joined-up approach to the cross-border implementation of PSD2, recommendations should be made to mandate a common approach to the implementation of PSD2 in Member States and Associated Countries in accordance with the objectives of the DG Internal Market. This falls short of transforming the directive into a regulation which would be a more extensive process and would undoubtedly take longer.
- To ensure interoperability between the different approaches to open banking access across Europe (and globally), recommendations should be made on harmonising APIs created by the various national/regional open banking organisations in Europe, such as the Open Banking Implementation Entity (OBIE), The Berlin Group et al<sup>146</sup>. In addition, it is vital that a common European approach to harmonising standards is taken to a global level, principally with FAPI<sup>147</sup> which is gaining currency in the USA, Japan and Australia.
- To ensure that authentication mechanisms across Europe are based on the same levels of security – which is not the case today – and to supplement the introduction of SCA in 2019, it is recommended that European level banking associations, the EBA in particular, enjoin with standards and other industry bodies to examine how banking security policies are aligned and steer best practices. Start-ups and SMEs in general can't offer the same level of security as a bank and could be ideal targets for an attack when in possession of customer data. Bad actors may also imitate FinTech companies in new variants of phishing attacks.

*Tools:* To achieve the policy changes recommended here is not envisaged that any tools are applicable except in the case of examining the existing security policies of participating banking/financial institutions, particularly those that share a common approach to access APIs.

### 3.8.4 Challenge 4: Convenient and compliant authentication

*Method:* With the introduction of open banking, users are having to engage with new and unfamiliar mechanisms for processing payments and allowing access to their banking assets. To improve the user experience in the use of open banking and thereby promote the uptake of open banking, the approach is to simplify and as far as possible harmonise user-oriented interfaces and tools, without loss of functionality

*Mechanism:* To identify the scenarios whereby users might be asked to provide third party access and make recommendations to regulators, and financial community stakeholders to collaborate with user groups and UX designers in modelling and implementing a standardised, language-independent approach to user-

---

<sup>146</sup> These include similar initiatives such as those in [Poland](#), [Slovenia](#) and [France](#).

<sup>147</sup> [Financial-grade API \(FAPI\)](#) is an industry-led specification of JSON data schemas, security and privacy protocols to support use cases for commercial and investment banking accounts as well as insurance and credit card accounts.

oriented interfaces and tools, that in so doing provide users with confidence that it is also GDPR compliant.<sup>148</sup>

*Tools:* A number of tools address different aspects of this challenge: Mobile pABC<sup>149</sup> (D3.1, Section 5.1), HAMSTERS, PetShop (D3.1, Section 3.6), Guidelines for GDPR compliant user experience (D3.1, Section 3.7)

### 3.8.5 Challenge 5: Real time revocation of right of access

*Method:* One of the benefits of PSD2 is being able to pass on the ‘right of access’ but it is also a potential loophole. Given some of the ambiguities in the regulatory language, particularly with respect to the timing of notification, a cross-border infrastructure is proposed that is able to carry out real time non-intrusive actions including the analysis, detection, and communication when a bad actor is detected.

*Mechanism:* The approach requires a series of real time actions on encrypted personal banking-related data to be carried out, using homomorphic encryption / secure multiparty computation (SMPC).

*Tools:* Sharemind MPC – Privacy-preserving data analysis (D3.2 – section 10.2).

### 3.8.6 Challenge 6: Corporate open banking security

*Method:* Open Banking does not only concern lending institutions, banks and FinTechs: the financial services industry is also making use of the possibilities afforded by API-based banking. Just as PSD2 does not cover all aspects of the end-to-end process for B2C financial transactions, the limitation also applies to B2B solutions. So not surprisingly, the approach to be taken is similar to that in Challenge 1, and requires a mapping of all transaction processes, taking into account both internal and external systems, and involving all stakeholders in B2B banking and payments including corporate users and applications.

*Mechanism:* To carry out an end-to-end risk analysis requires identifying a small number of financial institutions and to choose a set of processes that are representative of a range of transactions of varying degrees of complexity that traverse the whole eco-system including multiple actors.

*Tools:* There are a variety of general purpose and task-specific tools that would help the initial analysis, such as CORAS, HERMES, OFMC/AIF (all three D3.2, Section 5.2) and others, such as Testing, verification and mitigation methodology, SPARTA (both D3.1, Section 5.4), that could be used to monitor and assess the risk points and take action when vulnerabilities are detected.

Table 2: Challenges identified in the Open Banking vertical and tools needed to address them

Challenge	Tools/methods required	Tools/methods contemplated for Open Banking	Tools/methods that need to be addressed

<sup>148</sup> Although clearly impactful on Open Banking, this solution is not virtual specific.

<sup>149</sup> ABC stands for Attribute-Based Credentials

Challenge 1	End-to-end processing	Mapping end-to-end processes, taking into account both internal and external systems, involving all stakeholders in B2C banking and payment transactions including users. DP analysers, Security & Privacy by Design (both D3.1, Section 5.1), OFMC/AIF, CORAS (both D3.1, Section 5.2)	Having identified the security and privacy gaps in the end-to-end banking/financial processing chains, a further set of tools will be required to monitor and assess the risk points.
Challenge 2	Severing relationships	A systematic security analysis, modelling and implementation of solutions using modern methods to cover a number of scenarios that are not covered by legislation Trust Monitor (D3.1, Section 5.1)	Improved communication between authorities and financial institutions to protect the integrity of the banking/financial ecosystem in case of disruption.
Challenge 3	Harmonisation of national legislation	Policy recommendations on PSD2 to the EC's DG Internal Market	Enhancements on PSD2 legislation to achieve greater harmony on Member State implementation of the directive.
Challenge 3	Harmonisation of access mechanisms	Policy recommendations on harmonising APIs to national/regional open banking organisations, such as OBIE, The Berlin Group et al.	Pan-European agreements to ensure interoperability between the different approaches to open banking access across Europe (and globally)
Challenge 3	Harmonisation of security controls	Policy recommendations to banking associations, starting with the EBA, and participation in standards bodies	A pan-European agreement to ensure that authentication mechanisms across Europe are based on the same levels of security
Challenge 4	Improving the user experience	Recommendation to regulators, and financial community stakeholders to collaborate with user groups and UX designers Mobile pABC (D3.1, Section 5.1), HAMSTERS, PetShop (D3.1, Section 3.6), Guidelines for GDPR compliant user experience (D3.1, Section 3.7)	To simplify the user experience in using open banking user-oriented interfaces and tools without loss of functionality
Challenge 5	Production of statistics on distributed revocation requests	Data analysis of any encrypted personal banking-related data using homomorphic encryption / secure multiparty computation (SMPC) Sharemind MPC – Privacy-preserving data analysis (D3.2 – section 10.2)	Changes to the legislation should be recommended to tighten up the apparent loopholes regarding revocation of consent.

Challenge 6	Mitigation of corporate risks	Similar to Challenge 1, mapping end-to-end processes, taking into account both internal and external systems, involving all stakeholders in B2B banking and payment transactions including corporate users. CORAS, HERMES, OFMC/AIF (all D3.1, Section 5.1), Testing, verification and mitigation methodology, SPARTA (both D3.1, Section 5.4)	Having identified the security and privacy gaps in the end-to-end B2B transaction processing, a further set of tools will be required to monitor and assess the risk points and take action when vulnerabilities are detected.
-------------	-------------------------------	---	--

## 3.9 Roadmap

### 3.9.1 Short-term plan

Based on the ambitions of the demonstrator use cases in WP5, we would like to see the following objectives accomplished:

- The results of the fighting fraud experiments carried out under OBSIDIAN (Open Banking Sensitive Data Sharing Network for Europe) and CYTILIS (Cyber Threat Intelligence and Information Sharing) to point the way to the sharing of key data about fraudsters between banks in as near real time as possible, with the validation of national and/or supranational finance bodies
- Ideally, we should also be able to see results in cross-border data sharing scenarios, as well as where a reasonable subset of personal data (i.e. not only IBANs) is shared pseudonymously, which would also facilitate transparent eKYC for (non-fraudulent) customers wishing to set up secondary bank or payment accounts.
- The uptake of the use of a smartphone as a wallet to store not only cryptographic means, such as W3C WebAuthn and FIDO2,<sup>150</sup> but also to store and manage different verifiable credentials from a variety of reliable sources for authenticating onboarding customers by the banking community.

### 3.9.2 Beyond the end of the project plan

#### 3.9.2.1 Security 2025

Many of the challenges identified in previous roadmaps have still not been addressed or resolved and for the success of Open Banking in the short, medium and long term, these become vital and include:

- The whole end-to-end Open Banking process. This is to be mapped by drawing a map of all the stakeholders involved, how they interact, how they rely on each other and how the chain of trust is constructed. From this, it is to be expected that several gaps in security and privacy will become

<sup>150</sup><https://fidoalliance.org/fido2/>

apparent, leading to a variety of methods and approaches to ensure closure (see sections 3.6.12 and 3.8.1).

- The impact of the discontinuation of relationships in an established trust chain across the various scenarios envisaged above
- The technical and non-technical consequences of the mapping exercise in cross-border scenarios, including one-to-one, one-to-many and many-to-many, and beyond that across different jurisdiction based on the challenges as outlined in sections 3.6.14 and 3.8.3

In addition, we would like to see an agreed and working mechanism for participants in the international Open Banking ecosystem to collaborate. Unfortunately, this community missed out on achieving a single standard at first, and there is a strong case to be made for not seeking one now. Far better would be to build hubs that would enable different APIs, etc., to integrate seamlessly – a suitable comparison is the way that different styles of plugs work with adaptors universally without causing disruption or division.

### 3.9.2.2 Security 2030

Many of the challenges identified in previous roadmaps have still not been addressed or resolved and for the future success of Open Banking not only in the short term but also in the medium (2025) and long (2030) term, these become vital. Ideally, and optimistically, these targets could (and should) be achieved sooner than the timelines indicated here but other realities, including funding, and other apparent priorities have a habit of interfering.

- Improved third-party authentication/registration process with Member States' National Competent Authorities, especially in a cross-border context (see recent 1 MEUR open banking fraud between Hungary and the Netherlands)
- Connectivity of eIDAS111 certificates (with seals and transport certificates as required by regulation) with emerging PSD2-specific directory services
- Old “credential sharing” and “screen scraping” technologies (as permitted in PSD2 regulation under certain circumstances) versus modern methodologies (two-factor/SCA) and modern cyber-attacks (especially man-in-the-middle)
- Role of mobile ecosystem (apps, authentication, biometrics, wireless data, etc.) in PSD2 security
- Issue of “consent” under GDPR within PSD2: roles/liabilities of actors, conflicts between privacy and payment regulations, need for separate/neutral consent platforms at neither bank nor TPP

Risks in the planned next steps in Europe, especially the API “scheme” and new “rich POS solutions” triggering instant credit transfers (with irrevocable fund transfer and limited time to do full AML/KYC/FATCA/sanction checks) at physical and virtual e-commerce and m-commerce.

### 3.9.3 Milestones

By the end of the project, presented, or demonstrated ideally, at the end of project conference:

- Working prototypes based on OBSIDIAN network implemented and tested
- Working prototypes based on CYTILIS implemented and tested
- Working prototypes based on VCUCIM implemented and tested

- An Open Banking workshop/event (in 2H2022) with representatives from the financial community from several Member States and other countries as well as representatives of regulatory and trade bodies.

### 3.10 Summary

Since the last report, the uptake of Open Banking by financial institutions, merchants and FinTechs has gathered more momentum, but still has some way to go. By contrast, progress with rolling out RTS SCA has been slower than would have been anticipated or hoped for. Fortunately, the Open Banking ecosystem has not been disrupted by cyberattacks – at least for the time being.

As outlined in section 3.1, Europe has led the way in modernising payment services to the benefit of consumers and businesses through its payment service directives, specifically PSD2, which has opened up opportunities for new market players (i) to enable innovative services, (ii) to provide greater transparency and consumer choice, and (iii) to promote the digital single market within the EU and EEA. It also aimed at guaranteeing a high level of security, but as demonstrated, despite the introduction of RTS SCA, there are still considerable weaknesses in the transition from the traditional approaches to banking and payments to the transformative promises of Open Banking. One transparent conundrum is manifested in the apparent contradiction between the aims of PSD2 and the GDPR: both seek to protect the interests of consumers, the one by making financial data more accessible to third parties, the other by restricting the unconsented use of consumer data.

Our SWOT analysis (in section 3.6.2) indicates that, (i) although there are demonstrable weaknesses and threats, Europe is still in a strong position in terms of market leadership, and (ii) that the opportunities associated with ensuring the success of Open Banking are very encouraging, providing the EU and the other major European institutions a way to address the security and perception shortcomings.

In order to tackle the issues related to achieving greater security in Open Banking, we identify six main challenges:

- Challenge 1: Mapping of stakeholder interaction in end-to-end Open Banking processing
- Challenge 2: Setting up and discontinuing business relationships
- Challenge 3: Cross-border cooperation under differing legislation and security controls
- Challenge 4: Convenient and compliant authentication
- Challenge 5: Real time revocation of right of access
- Challenge 6: Corporate open banking security

It will be important to address these challenges over the coming years, not least to ensure that the progress of the Open Banking initiative doesn't falter, either through lack of European-wide coordination in certification processes and API development or through other global initiatives superseding the considerable amount of work carried out to date, which would be a blow to European Digital Sovereignty. There is still a hesitancy by many organisations in fully embracing Open Banking due to the potential risks, both financial and brand-related, and ambiguities surrounding liability.



## 4 Supply Chain Security Assurance

### 4.1 The Big Picture

A supply chain can be seen as a globally distributed and interconnected network of stakeholders, processes, functions, information, and resources involved in the creation and distribution of a product: from the delivery of basic materials from the supplier to the manufacturer, up to the end user. Supply chain ecosystems are extremely complex: One particular end product or good – which can be physical (e.g. a photovoltaic plate), digital (e.g. a smart grid software component), or a combination of both – is the result of the interactions between multiple tiers of public and private stakeholders (e.g. manufacturers, suppliers, integrators, end consumers, supervisory agencies). These interactions involve various processes, including the transport of all components and goods, the tracing of their location, guaranteeing the quality and integrity of all parts and products, accrediting the technical and organizational competence of all stakeholders, and identifying and resolving potential issues or conflicts. Moreover, we need to consider that supply chain ecosystems are highly heterogeneous, as the complexity and requirements in the management of all goods (from bicycles to planes, from web software components to power plant software architectures) are different.

The supply chain ecosystem is also evolving due to the integration of information technologies (IT) with the existing operational technologies (OT) infrastructures. The integration of these new “digital and ICT<sup>151</sup>” elements across all value chains requires additional processes and functions, including monitoring the state and performance across production plants, transportation systems, and warehouses in real-time using diverse technologies (sensors, 4G/5G connections), sharing information and processes between different stakeholders (from certification information to the state of assets and goods) in a digital space, and complying with additional technical and regulatory requirements. Although digitalisation increases the complexity of this ecosystem, it also brings numerous benefits, including monitoring the compliance and state of transported parts and goods, pushing forward just-in-time production, predicting and understanding problems, solving disputes in a timely manner, and so on.

### 4.2 Overview

It would not be an overstatement to declare that the complex interconnected web of assets, services, and actors that make up the various supply chain networks that exist in the world is one of the core foundations of our modern society. Not only our economies but also our daily lives depend heavily on it. Thanks to supply chain infrastructures being considered as critical infrastructures, since 2001, there have been a multitude of recommendations and standards in this area. Such standards mainly define procedures and best practices, which focus on aspects such as the integration of traditional security procedures, how to perform risk analyses to make decisions and create contingency plans, and the management of the interactions between suppliers and providers.

However, the complexity of the supply chain ecosystem, which incorporates more and more IT, makes the protection of each of its elements extremely difficult, even almost impossible. As the saying goes, “Security

---

<sup>151</sup> ICT stands for Information and Communication Technologies

is as strong as its weakest link”. In fact, the number and impact of attacks that specifically target supply chains is on the rise. These attacks are not only IT-based attacks, like the manipulation of software components to introduce vulnerabilities that can be exploited in the future, but also physical, such as manipulating the supply chain processes to introduce counterfeit or tampered goods. The protection of this interconnected supply chain web against these and other attacks needs to go one step further.

However, according to various analyses performed in the last few years, the literature on supply chain security has become relatively stagnant. It is then necessary to perform a proper analysis of the main (research) challenges that must be tackled in order to protect this interconnected supply chain web. As supply chains are highly dependent on IT technologies, some of these challenges are related to the protection of these IT infrastructures, or even to the integration of novel IT technologies (e.g. blockchain) to provide an additional layer of protection. Thus, it may be possible to make use of the existing literature on the protection of IT and OT infrastructures to explore the mechanisms and tools that could be applied to protect the supply chain ecosystem.

## 4.3 What is at stake?

### 4.3.1 What needs to be protected?

At present, no standard or report provides a complete taxonomy that describes all the actors, services and assets that should be considered as critical in supply chain scenarios. Nevertheless, it is possible to create a taxonomy that fulfils that requirement by extracting information from this multitude of standards and reports. Note that this taxonomy takes into consideration the dual nature of existing supply chains, where the **goods** that are managed and processed within the supply chain can be either physical or digital, and where data and algorithms – which are used to build the software – are the equivalent of raw materials and production processes in a software supply chain.

The main **actors** that interact with each other in supply chain scenarios can be mainly derived from the Open Trusted Technology Provider Standard (O-TTPS) v1.1, plus other standards like the ISO 28000 [ISO 2019] series that focus more on physical supply chains. The main categories are *Customers* (end users, acquirers), *(Re)sellers* (retailers, wholesalers), *Vendors / Providers* (including system integrators), *Suppliers*, and *Supporting actors* (logistic providers, standards bodies, certification / accreditation bodies). Note that one actor can fit into more than one category. For example, a supplier can also be a provider.

As for the main **services** provided within the supply chain ecosystem, they can be classified as follows:

- *Production services*: Sourcing / Processing of materials, Design / Development, Fabrication / Manufacturing.
- *Transportation services*: Packaging / Labelling, Shipment, Traceability, Distribution / Delivery.
- *Usage services*: Quality and test management, Installation, Operation, Maintenance.
- *Business services*: Market research, Sales promotion, Technical studies.
- *Supporting services*: Storage and archival of information, Product and vendor certification.

As for the **assets** that comprise the supply chain ecosystem, the following taxonomy is based on the ENISA taxonomy for maritime transport [ENISA 2019] and focuses on assets that are owned and/or managed by the different actors that comprise the supply chain vertical, not including assets that belong

to other critical infrastructure sectors. These assets can be classified into *Fixed Infrastructure* (buildings, other supporting infrastructures), *Mobile Infrastructure* (transport vehicles, mechanical handling equipment), *Goods and Logistic Units* (goods, services, labels, pallets, bulk logistic units, small logistic units), *IT Infrastructures* (e.g. cyber-physical systems), *IT Systems* (e.g. enterprise resource planning (ERP) systems), *IT End-Devices* (e.g. workstations, mobile devices, Sensors, RFID labels...), *IT Networks and components* (facilities networks, supply chain collaboration networks, network components), *OT Systems and Networks* (e.g. “industrial” control systems), *OT End-Devices* (e.g. sourcing and processing machinery, manufacturing machinery, cargo handling systems), *Safety and Security Systems* (e.g. detection and alerting systems, access control systems), *People* (including internal and external staff), and *Information and Data* (e.g. intellectual property, transport data, enterprise agreements).

### 4.3.2 What is expected to go wrong?

Common threats reported against the supply chain (both physical and digital) are extracted from existing reports and state of the art analyses. They can be found at any stage of the supply chain ecosystem (from design and manufacturing to deployment and maintenance) and are summarized in the following threat landscape:

- General threats:
  - Sabotage (both physical and digital), cascade effects, export control violations, overall corruption, service disruption, insider threats (both physical and digital).
- Specific goods threats:
  - Manipulation of goods (including packaging, labelling, and production metadata), counterfeited goods, use of unauthorized/sub-par parts, unauthorized configurations, poor manufacturing and development practices, inventory theft.
- Specific information systems threats:
  - Traditional cyberattacks (e.g. malware), data breach (e.g. loss of intellectual property), information distortion, (un)intentional vulnerabilities, malicious updates/maintenance.
- Specific transportation threats:
  - Piracy, smuggling

In addition, new emerging technologies have increased the number of potential infiltration points adversaries can target, and as a result, will pose new threats to this particular ecosystem:

- The advent of **Industry 4.0** and the integration of **cyber-physical systems (CPS)** will dilute the barriers between IT and OT systems. As a result, it will facilitate the emergence of several IT attack vectors that specifically target industrial ecosystems.
- By delegating more services and infrastructures to the **cloud**, supply chain systems inherit the threats that already target that space, such as information and service theft (e.g. through virtualization vulnerabilities) and infrastructure availability.
- The **Internet of Things (IoT)** facilitates the interconnection of any entity and an almost real-time acquisition and processing of information, but at the same time facilitates the execution of cyberattacks targeting any internet-connected entity (from goods to vehicles or infrastructures),

anywhere and anytime in the world. However, note that remote cyberattacks are not the only attacks that can be launched against this technology. For example, faulty sensors can provide wrong information about the state of a supply chain process.

Moreover, beyond the interconnection of systems and the adaptation of computing technologies, the digitization of all industrial processes also leads to other and new research challenges and risks:

- **Artificial intelligence** injects autonomy and intelligence into production and distribution processes, but it will also become a source of new security risks. For example, attackers might modify the logic of AI Supply Chain processes by altering the training phases (and their samples) and their outputs.
- **Big Data** is being used to perform computations on large volumes of data, and the results of their analyses can be relevant to improve the logistics of a Supply Chain. However, the risks increase when there is no clear access policy and privacy controls, plus the misuse of these techniques might bring numerous privacy issues.
- **Augmented and virtual reality** are great Industry 4.0 technologies, as they enable human operators to make decisions and act according to what they see or feel. Yet if digital reality does not match physical reality, multiple security risks might arise, which may cause incorrect and invalid decisions, and inappropriate actions.
- **Digital twins**, or digital counterparts of physical objects / processes<sup>152</sup>, are certainly one of the great fourth-generation industrial-level technological discoveries, but also a double-edged sword. Its power to control the physical world through its bidirectional interfaces will expand the attack surfaces (digital world to physical world, and vice versa), and add new security risks.

Finally, we must note that a supply chain attack can be performed either *intentional* or *unintentional*:

- For example, Asus was hit by an intentional supply chain attack in early 2019: It happened via malicious code in a software update tool where “[...] a small number of devices has been implanted with malicious code through a sophisticated attack on our Live Update servers in an attempt to target a very small and specific user group”<sup>153</sup>.
- In 2018, Ericsson suffered from an unintentional supply chain attack: An expired certificate on Ericsson devices/software – “[...] because of a faulty software [...]”<sup>154</sup> – caused network outage and affected millions of inhabitants across Europe and Asia. Imagine, if this was intentional and planned perfectly with a ground invasion then this could be a disastrous national security problem.

### 4.3.3 What is the worst thing that can happen?

For the supply chain case, we have considered the incidents presented in this and other sections, and how they could affect our society if no further research is done in this area. We also have considered the potential cascade effects that a failure of the supply chain would cause in our society.

---

<sup>152</sup> <https://csrc.nist.gov/publications/detail/nistir/8356/draft>

<sup>153</sup> <https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/>

<sup>154</sup> <https://www.ericsson.com/en/press-releases/2018/12/update-on-software-issue-impacting-certain-customers>

To evaluate the impact on each asset, the following three characteristics are considered:

- *Confidentiality*: Any kind of physical/digital information managed and/or produced by the supply chain ecosystem or goods are stolen.
- *Integrity*: The integrity of any of the assets (from services to actors) is compromised, where such compromise can stay hidden while being exploited constantly.
- *Availability*: Any assets (from services to actors), including goods, are lost, and maybe unrecoverable.

- As a result, the worst types of impact provided by NIST [NIST 2012] and identified in the supply chain case are the following:

- **Harm to Operations:**

- *Inability to perform current missions/business functions*: attacks through the supply chain become commonplace, and organizations are always vulnerable.
- *Inability, or limited ability, to perform missions/business functions in the future*: as organizations are always vulnerable, it becomes impossible to fully recover from continuous attacks.
- *Harms (e.g. financial costs, sanctions) due to noncompliance*: complex regulations cannot be implemented.
- *Relational harms*: Trust relationships between organizations are lost, because managing the supply chain threats has become an impossible task.

- **Harm to Assets:**

- *Damage to or loss of physical facilities*: terrorist attacks take advantage of supply chain vulnerabilities to damage physical facilities, also causing human casualties.
- *Damage to or loss of information systems or networks*: traditional cyber-attacks, such as ransomware, relentlessly disable the underlying IT infrastructure that supports the supply chain ecosystem.
- *Damage to or loss of component parts or supplies*: it becomes impossible to manage the threats against physical/digital assets when the supply chain is transformed into a chaotic supply web.
- *Damage to or loss of information assets*: Various information assets are tampered with by malicious adversaries rendering the knowhow and intellectual property of companies useless.
- *Loss of intellectual property*: IP routinely gets stolen from corporations and governments.

- **Harm to Individuals:**

- *Injury or loss of life*: counterfeited or altered products affect people either directly or indirectly.
- *Physical or psychological mistreatment*: the public cannot trust the safety of the products they use in their daily lives.

- **Harm to other organizations:**

- *Relational harms*: The interconnected nature of supply chains causes damage to all actors involved in this vertical if the ecosystem can no longer be trusted.

- **Harm to the Nation**

- *Relational harms*: loss of trust relationships with other nations, loss of national reputation, loss of national security due to the impact on the critical infrastructure.

## 4.4 Who are the attackers?

As mentioned in deliverable D4.1 and throughout this section, the Supply Chain is one of the most extended and oldest sectors, having seen four distinct industrial generations until arriving at the 4th Industrial Revolution, commonly known today as Industry 4.0. Through this new revolution, industries are now able to couple the new IT in the operational processes and their technologies (also known as OT), thus allowing the convergence of IT networks to OT networks (IT-OT). However, this technological convergence, together with the globalization of the sector and its current influence on the other verticals (e.g. medical, maritime) makes it a very vulnerable ecosystem, which is targeted by numerous attackers.

For this section, we have analysed how the different agent profiles have targeted supply chain scenarios. In particular, *criminal organizations* have focused mostly on the smuggling of people<sup>155</sup>, weapons, and illegal substances<sup>156 157</sup>, theft<sup>158</sup>, and various digital threats such as digital skimming<sup>159</sup> and theft of personal information<sup>160</sup>. *Terrorists* have also tried to abuse the supply chain to perform acts of terror<sup>161</sup>. All *intelligence services* have also participated in the manipulation of the products and services of both hardware<sup>162</sup> and software<sup>163</sup> supply chain, for various purposes such as personal and industrial espionage and sabotage. Last but not least, various *supply chain actors* have also acted as insiders, causing problems in the supply chain due to product manipulation / mismanagement<sup>164</sup>.

As a result of our analyses, we have observed that supply chain threats are linked to theft, terrorism, counterfeit products, product manipulation or adulteration, smuggling of illegal goods, weapons or people, illicit use and acquisition of data for espionage or disclosure, and sabotage. However, as shown by the ENISA Threat Landscape for Supply Chain Attacks, published in 2021<sup>165</sup>, most threats nowadays are

<sup>155</sup><https://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8124226/Cargo-plane-bomb-plot-ink-cartridge-bomb-timed-to-blow-up-over-US.html>

<sup>156</sup><https://www.bbc.com/news/world-europe-25640485>

<sup>157</sup><https://www.bbc.com/news/world-europe-24539417>

<sup>158</sup>[https://onlinelibrary.wiley.com/doi/pdf/10.1111/deci.12336?casa\\_token=ifPZDxYdAwQAAAAA:jU0gYtsIT0fFOJOT3V5ozqHZOrtQW328jTZsVuK16QCQhBuSPFAeasxZtfSkqVQQ1enFvcBHASnXFXE](https://onlinelibrary.wiley.com/doi/pdf/10.1111/deci.12336?casa_token=ifPZDxYdAwQAAAAA:jU0gYtsIT0fFOJOT3V5ozqHZOrtQW328jTZsVuK16QCQhBuSPFAeasxZtfSkqVQQ1enFvcBHASnXFXE)

<sup>159</sup><https://blog.trendmicro.com/trendlabs-security-intelligence/new-magecart-attack-delivered-through-compromised-advertising-supply-chain/>

<sup>160</sup><https://research.checkpoint.com/2019/operation-sheep-pilfer-analytics-sdk-in-action/>

<sup>161</sup><https://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8124226/Cargo-plane-bomb-plot-ink-cartridge-bomb-timed-to-blow-up-over-US.html>

<sup>162</sup><https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies>

<sup>163</sup><https://carnegieendowment.org/2019/10/04/ict-supply-chain-integrity-principles-for-governmental-and-corporate-policies-pub-79974>

<https://www.reuters.com/article/us-cyber-attack-ukraine-backdoor/ukraine-scrambles-to-contain-new-cyber-threat-after-notpetya-attack-idUSKBN19Q14P>

<sup>164</sup><https://www.theguardian.com/uk/2013/feb/15/horsemeat-scandal-the-essential-guide#101>

<sup>165</sup> ENISA, Threat Landscape for Supply Chain Attacks. July 2021, <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>

focused on the acquisition of data, which also can result in sabotage and theft. Examples of some of these threats are shown in the next section.

## 4.5 Major incidents in this vertical

Here, we present a list of cyber-attacks on supply chains. The list includes a cross-section of more notable, recent, and different types of attacks on supply chains across different industries. The list by no means presents an exhaustive account of attacks on supply chains. After all, ENISA, in its 2021 threat report, estimated that there have been four times as many attacks on supply chains in 2021 as there were in 2020.<sup>166</sup>

- *Kaseya cyberattack (2021; theft)*<sup>167</sup>: Kaseya provides IT solutions, including a remote-monitoring and management tool for handling networks and endpoints (designed for, among others, managed service providers, which amplified the attack by exposing their customers). The attack compromised this solution (they circumvented authentication controls) in a way that allowed the attackers to distribute malicious payload through hosts managed by the software. The attacker used this to distribute ransomware, reportedly affecting over a thousand businesses. The REvil ransomware group took credit for the attack.
- *Mimecast cyberattack (2021; acquisition of data)*<sup>168</sup>: Mimecast provides email security services (backup, spam and phishing protection) for Microsoft 365. In the attack, the certificates required for verification and authentication by Mimecast's servers were compromised, allowing the attackers to eavesdrop on the communication and retrieve data from the mailboxes. The Russian hacking group APT29 is believed to be responsible for the attack.
- *Codecov breach (2021; acquisition of data)*<sup>169</sup>: Codecov produces code coverage and software testing tools. The attackers managed to gain access to the continuous integration environments and were able to extract all data (e.g. data on databases, payment systems, credentials, etc.) from the code Codecov's customers were testing. It is currently unknown who was responsible for the attack.
- *Colonial Pipeline breach (2021; acquisition of data, sabotage)*<sup>170</sup>: Attackers gained access to the Colonial Pipeline network through no longer used credentials, most likely obtained on the dark web. After stealing the data from the company, the attackers started a ransomware attack, forcing the company to shut down its fuel pipeline, which provides almost half of all the fuel on the east coast of the United States of America. Criminal hacking group DarkSide was identified as responsible for the attack.
- *SITA breach (2021; acquisition of data)*<sup>171</sup>: SITA handles many online services for nearly all the world's major airlines. As a consequence of a breach, many airlines (SITA has about 90% of the

---

<sup>166</sup> <https://blog.checkpoint.com/2021/10/26/deepfakes-cryptocurrency-and-mobile-wallets-cybercriminals-find-new-opportunities-in-2022>

<sup>167</sup> <https://helpdesk.kaseya.com/hc/en-gb/articles/4403584098961-Incident-Overview-Technical-Details>

<sup>168</sup> <https://www.mimecast.com/incident-report/>

<sup>169</sup> <https://www.reuters.com/technology/us-investigators-probing-breach-san-francisco-code-testing-company-firm-2021-04-16>

<sup>170</sup> <https://www.cisa.gov/uscert/ncas/alerts/aa21-131a>

<sup>171</sup> <https://www.incibe-cert.es/en/early-warning/cybersecurity-highlights/data-breach-sita-affects-multiple-airlines>

world's airlines as its clients) have had the data on their customers stolen. The attackers have not been confirmed, but it is believed it was the China-backed cyber threat group APT41.

- *SolarWinds cyberattack (2020; acquisition of data)*<sup>172</sup>: SolarWinds builds monitoring and management tools. Attackers managed to gain access to the company's network and introduced malicious code into the system. When SolarWinds then sent out updates for its systems, it unwittingly distributed this malicious code to its customers. The code created a backdoor to the customer's network, granting them access to install even more malware that helped them spy on companies and organizations. Authorities have blamed the hacking group APT29 for the attack.
- *NotPetya (2017; sabotage)*<sup>173</sup>: NotPetya was one of the most devastating malware attacks that primarily targeted Ukraine but spread well beyond it. One of the many affected was Maersk, the world largest shipper of containers. The attack ruined most of the computers in their network. The company could no longer tell what was in any of the shipping containers on any of the ships and was subsequently forced to halt most of its operations. NotPetya appeared as ransomware, but there was no actual way to recover the data. The Russian Sandworm hacking group within the GRU was blamed for the attack. Shipping, in general, has been targeted more often in recent years.
- *JBS USA cyberattack (2021; acquisition of data, sabotage)*<sup>174</sup>: In May 2021, cyber actors using a variant of the Sodinokibi/REvil ransomware compromised computer networks in the US and overseas locations of a global meat processing company, which resulted in the possible exfiltration of company data and the shutdown of some US-based plants for several days. The temporary shutdown reduced the number of cattle and hogs slaughtered, causing a shortage in the US meat supply and driving wholesale meat prices up as much as 25 per cent, according to open source reports.

## 4.6 Research Challenges

### 4.6.1 State of the Art

The second version of the CyberSec4Europe “*Research and Development Roadmap*” [Markatos 2021] provided an overview of the results of research into the state of the art of supply chain security with respect to all research challenges. As with other verticals, in this version of the “*Research and Development Roadmap*”, this subsection updates that state of the art with new content from 2021, related to the new advances and research results.

#### 4.6.1.1 Supply chain risks, vulnerabilities and resilience

For any company, it is essential to implement various supply chain risk management (SCRM) strategies, so that it may be continuously aware of the existence of potential risks—both everyday and exceptional—to its supply chains. Such awareness can allow companies to prevent and react against these flaws, and provide solutions before business continuity gets affected. In turn, SCRM is closely intertwined with supply chain vulnerabilities (SCV) and supply chain resilience (SCRES) [JK 2011]: SCRM enhances resilience by

<sup>172</sup> <https://www.cynet.com/attack-techniques-hands-on/sunburst-backdoor-c2-communication-protocol/>

<sup>173</sup> Monetary Impact on 8 public firms that were directly hit by NotPetya, stock value dropped by 5%: [https://www.newyorkfed.org/medialibrary/media/research/staff\\_reports/sr937.pdf](https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr937.pdf)

<sup>174</sup> <https://www.aha.org/system/files/media/file/2021/09/fbi-tlp-white-pin-cyber-criminal-actors-targeting-food-agriculture-sector-ansomware-attacks-9-1-21.pdf>

improving the flexibility, visibility, velocity and collaboration capabilities of supply chains. Moreover, the correct integration of SCRM strategies can decrease the overall vulnerability of supply chains to disruptive risk events [RP 2018].

As of 2021, various national and international standards and frameworks are being used by organisations to underpin their internal SCRM policies and practices. Some of these standards are relevant to specific sectors, such as the automotive sector (IATF 16949:2016 [IATF16949 2016]) and electric systems [NERC 2017]. Other standards, such as ISO 31000:2018 [ISO31000 2018] and the various NIST Special Publications, such as NIST SP 800-161 (currently under revision, cf. [NIST 2021]) and NIST 800-53 Rev. 5 [NIST 2020b], provide the foundation to manage risks in supply chain ecosystems. These standards consider not only cybersecurity vulnerabilities, but also other issues, such as counterfeits and natural disasters, to name but a few. Moreover, organisations may also require their business partners to comply with specific cybersecurity standards, such as the ISO/IEC 27000 series of standards [ISO/IEC27000 2018].

Clearly, it is essential to consider cybersecurity as a crucially important factor in the development of risk and vulnerability strategies. From the analysis of the different cyber threat landscape reports authored by governmental organizations like ENISA [ENISA 2021C] and private companies like Accenture<sup>175</sup>, it can be concluded that the number of cyberattacks that target supply chain infrastructures (in both the physical and the digital world) is continuously increasing, and could even destroy business continuity if left unchecked<sup>176</sup>. This situation facilitates the creation of additional guidelines, such as the ENISA “*Secure supply chain for IoT*” guidelines [ENISA 2020C], which provide additional good practices based on existing standards and research.

However, it is still necessary to integrate more tools that facilitate the management of cybersecurity risks in the context of supply chains. That is why, as shown in the next paragraphs, there have been various concepts that focus on the integration of cybersecurity and risk/vulnerability analysis in supply chains, in both the military and civilian domains. These concepts can be applied at different levels: from the perspective of a single actor in the supply chain, where its interactions with Tier 1 suppliers and their assets can be analysed, to a more holistic view of a supply chain infrastructure, where multiple actors collaborate to create an overview of the relationships between several supply chain entities.

#### *Attack Trees/Graphs.*

One of the concepts that can be applied in this context is *attack trees/graphs*. These are conceptual diagrams that provide a formal way to describe systems security as a function of all possible conceivable attacks, where the root of the tree denotes an exploit and the leaves represent different actions to achieve that goal [NAD 2021]. By using these trees, it is possible to discover the most optimal attack paths (or kill chains) that can disrupt the different actors, services and assets of supply chains. As various elements of an attack path correspond to elements of a supply chain infrastructure, it is then possible to incorporate additional

---

<sup>175</sup> <https://www.accenture.com/acnmedia/pdf-107/accenture-security-cyber.pdf>

<sup>176</sup> <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

measures to prevent, protect, and react against cyberattacks. Moreover, it is possible to assess the risks of these attacks in order to prioritise the deployment of defence mechanisms.

There are various research works that apply the concept of attack trees in supply chains to specific industry verticals. For example, in [NFW 2017], the authors analyse the cyber kill chains that affect vehicle manufacturers and provide a formal vulnerability-analysis system that can propose minimum but essential measures for defence. Note, however, that this approach can only be applied by the vehicle manufacturer, as it focuses on an analysis of potential vulnerabilities within the vehicle components. Other works make use of attack trees to provide more effective protection to distributed complex IT infrastructures like the ones used in supply chain ecosystems. For example, in [NAD 2021], the authors make use of machine learning strategies to extract attack graphs directly from intrusion alerts caused by distributed multi-stage attacks, i.e. attacks caused by multiple adversaries compromising various targets

#### *Analysis of Cascading Failures.*

Another concept that can be applied in this context, which is also based on modelling interdependence graphs, is the *analysis of cascading failures*, also known as the cascade effect. This concept refers to accidental or malicious faults that can spread unpredictably in a highly interconnected ecosystem and may cause unexpected effects. This concept has actually been extensively studied, not only in supply chains [GJL 2020], but also in other related areas such as critical infrastructures [HSE 2018]. However, there are very few studies that analyse how to integrate cybersecurity and cascading failures in the context of supply chains, although their results are interesting. For example, in [PPK 2018], the authors provide a tool that incorporates cyber threats into the analysis of cascading scenarios modelled by dependency graphs. Moreover, the authors also use this tool to integrate cyber threats within risk-assessment processes, generating baseline security policies and identifying security controls that can be applied to the weakest links. Precisely, this work has evolved under the umbrella of the CS4E project, and new challenges and risks concerning cyber security in a supply chain environment have been identified [PPK 2021].

On the other hand, there are various works in the area of critical infrastructures, where cybersecurity is considered as an important factor in cascading failures. There are various examples of this. In [FCK 2017], the authors provide a distributed emulation and simulation platform for large-scale critical systems, which can be used to test the cascade effects caused by attacks against the infrastructure. In [vLJO+ 2019], the authors provide a preliminary study of how experts react against unexpected threats and cascade effects in interconnected critical infrastructures, and conclude that the severity of the cascade effect depends largely on the quality of the early crisis response and on cross-sectorial collaborations. Finally, in [PAN 2020], the authors point out that existing global frameworks to reduce disaster risks caused by cascading failures do not take cyber security risks into account, and such risks should be integrated into existing global policies. Therefore, all these research papers could be used as a starting point to improve the existing research into the impact of security on supply chain cascading failures.

#### **4.6.1.2 Attack prevention, detection and response in supply chains**

As mentioned in previous sections, the integration of **IT and OT** infrastructures in supply chains, under the umbrella of Industry 4.0, provides numerous advantages in terms of operational processes. Among its multiple advantages, we can distinguish the need to converge towards IT-OT networks and maximise industrial digitalisation processes through the new information technologies. The objective is not only to help to improve the quality of production and distribution services, but also to allow the industry to adjust

and optimise its products and sales according to real demand. Unfortunately, this technological expansion (IoT, cloud, CPS, AI, etc.) opens, in turn, the door to multiple kinds of attack on the supply chain, and leads to diverse security problems, many of them related to **confidentiality** (mainly in the theft of intellectual property), **integrity** and **availability** of the product life cycle and its value chain [CRF+ 2018].

So far, most of the proposed approaches to prevention, detection and response focus primarily on offering reactive methods rather than *proactive prevention approaches*, without going further and looking at how to avoid adverse situations in time, or how to eradicate or mitigate possible (collateral) effects [GSC+ 2017] [CRF+ 2018]. Some threats have already been contemplated in [CRF+ 2018], identifying possible malicious stakeholders and the problems that they may bring to the industrial ecosystem with the new technologies (e.g. vendors or customers might be interested in escalating privileges within the cloud). Additionally, some efforts are being made on developing well-prepared incident management processes that involve external partners [LAN 2021].

#### *Cloud Computing.*

Many of the technologies that are being adopted to improve the quality of the services and the optimisation of the value chain, can, in turn, be part of security mechanisms. One of the most extended technologies in scientific literature is precisely *cloud computing and its related paradigms* [CRF+ 2018] [O'RLM 2019] [HCG+ 2020]. The computational and storage capacities of these systems encourage designing or building effective solutions, the computation of which can be central or distributed within the system. This flexibility level helps security experts to deploy the main security actions in a cloud server or in a federated edge-to-cloud continuum (e.g. authentication [LSC 2015] [PSvS 2019], access control [LSH+ 2011] [PSvS 2019]) or distribute them throughout the entire system (e.g. distributed detection [HAP+ 2016], federated learning [AHM 2021]).

Clearly, working with powerful technologies such as cloud computing and edge computing requires further research, not only at the perimeter level but also at the computing and storage level—mainly because the edge-to-cloud continuum is vulnerable to compliance violations and cybersecurity issues [HCG+ 2020] [RAN 2021]. At perimeter level, Software Defined Networks could be a suitable mechanism to reduce an organisation's attack surface [O'RLM 2019] but also any other security mechanism with support to protect virtualisation infrastructures, and the access to private data can be essential in this new computing paradigm.

#### *Big Data.*

At the computing and storage level, the technology adds diverse advantages to collect, process and render large data volumes, which can be processed with *Big Data techniques*. Precisely, this field has surged in the last years, with multiple applications in the area of supply chains [POU 2021]. Among the utilities of Big Data and its related computation paradigms (machine-learning and data mining), it is worth highlighting its usefulness for decision-making and rapid actuation. These two primary functions (decision-making and rapid actuation) are partly due to the capacities of the current machine-learning models to manage data and predict deviations [ABH+ 2020], which can even be combined with other approaches to optimise their services and improve the quality and accuracy of the prevention processes (e.g. with data-driven approaches to order the sequence of events [KCK+ 2019]). Precisely, Big Data is closely interacting with the edge-to-cloud continuum to optimize the use of resources and to share information related to intrusion prevention,

in the context of federated learning [AHM 2021]. Still, the data life-cycle needs to be protected, as not only these techniques can be abused, but also the data sources can be poisoned in order to manipulate the results provided by Big Data techniques [GOLD 2021]. Bad use of these data warehouses can significantly impact on the privacy of an organisation or may alter the integrity of the data.

#### *Blockchain and Smart Contracts.*

*Blockchain* is another relevant technology that can be adapted to the Supply Chain sector for multiple proposals. As with Big Data, this field has surged in the last years, with multiple researchers exploring the applicability of this paradigm in the field of supply chains [LIM 2021]. The immutability features of this technology can help to improve or optimise the processes related to risk management and assessment, contingency plans, situational awareness and detection of potential threats, especially related with fraud in the Supply Chain [Min 2019]. The technology can also be combined with other existing ones, such as IIoT<sup>177</sup>/CPS/IoT, to create an interoperable and secure industrial environment. Precisely, Blockchain is being used as a foundation for the integration of attack detection and response systems. Its nature as a decentralized immutable storage makes it useful for the exchange of information between multiple partners, such as sharing of threat and vulnerability repositories [CSP+ 2020], and information related to federated learning [KHA 2021]. Still, more research is needed to identify both the opportunities and the limitations of Blockchain technology in the context of attack prevention and detection.

#### *Physically Unclonable Functions.*

*Physical/physically Unclonable Function (PUF)* are security primitive physical devices considered for the Supply Chain. Their main aim is to prevent the trade in counterfeit goods [HCG+ 2020], adding a hardware-based digital signature that works as a unique identifier for each device. This procedure complicates the forgery process, even for the manufacturers. In recent years, its application has exploded in many applications (IoT-enabled healthcare systems [GS 2020] or Unmanned Aerial Vehicles (UAVs) [GGK+ 2020]), including the Supply Chain, through the use of PUF-enabled RFID (Radio-Frequency Identification) devices that cannot be cloned [DAV 2021]. Current research challenges are mainly concentrated on how to improve the security of the technology, since its effectiveness depends on the facility with which an adversary may counterfeit objects without affecting the PUF itself. Also, the entire counterfeit detection process can be seriously affected if an adversary is able to extract the PUF from an object and install it within another device [HCG+ 2020]. We also should point out that some PUF-like approaches (analysis of unique properties) are being explored for raw materials [ABE 2021].

#### *Situational Awareness.*

One specific aspect of prevention, detection and response is precisely *situational awareness*. Its (perception, comprehension and projection) modules can be adapted for complex and dynamic contexts in order to: (i) perceive the states of a determined context (e.g. containers [VKL 2016]); (ii) understand the meaning of its context (through detection models and AI); and (iii) project the states, risks and consequences of the context in real-time (through forecasting models and traceability techniques, such as consensus, Opinion Dynamics [RRA 2019] or distributed clustering [RAR+ 2020]). This information can even be shared by several Supply

---

<sup>177</sup> IIoT stands for the Internet of Industrial Things

Chain partners to increase their level of resilience [KKV 2013] [ASA 2018] [YI 2019] [HAA 2021], reducing possible threat or business risks and improving their cyber intelligence in terms of decision-making for an accurate and trustworthy response. As stated in [BGS 2015], a typical goal of cyber intelligence is to establish facts that can later be used to build trustworthy and valid inferences (hypotheses, estimations, conclusions and/or predictions) that support decision making or operational actions such as detection, prevention and response. This kind of intelligence, and particularly Cyber Threat Intelligence (CTI), is being closely explored by a few authors [YI 2019] [HAA 2021] in the context of supply chains, but still more research is needed to create secure common access platforms to share events, threats, security risks and incidents.

### *Digital Twins.*

At this point, it is also worth highlighting the role of the *Digital Twin*. Its simulation capabilities help the underlying system or the organisation not only to optimise the behaviour of a system, process or product, but also to detect variations or deviations between the real and virtual worlds. In this sense, the Digital Twin can serve as a protection tool with the ability to anticipate anomalous states, behaviour and activities that can be critical to the real physical world [PKP 2020] [MYL 2021]. Research on this field is advancing at a steady pace, although not only more experiments are needed, but also it is necessary to understand the specific nuances of supply chain ecosystems. In addition, Digital Twin capabilities to replicate the real world and simulate environments foster the possibility to promote learning and training through cyber-range models (e.g. in Industry 4.0 [BFP+ 2018], Maritime [TMJ 2020] or industrial control scenarios [GF 2019], amongst others). Through these models, it would be possible to (i) show awareness in the different domains of a Supply Chain, (ii) stimulate education on cybersecurity, and (ii) provide feedback to other key protection systems, such as situational awareness, CTI platforms or risk assessment managers [VVO+ 2017] [VIE 2021]. This field of application of Digital Twins is also advancing at a steady pace.

#### **4.6.1.3 Data sharing in supply chain ecosystems**

In digital supply chains, it is essential to provide secure and trusted data sharing environments that will facilitate the exchange of information between supply chain actors. The existence of such environments has numerous benefits, such as creating new opportunities for business, optimising operational processes, reducing the administrative burden, and enhancing supply chain visibility and bundling capabilities. Precisely one of the major benefits of data sharing in supply chains is traceability. As we move physical and/or digital goods across space, it is essential to track the provenance and journey of all goods from the very start to the end. Through traceability, companies can meet regulatory requirements, connect with and understand the actions of all actors, and even ensure the reliability of sustainability claims (social, economic, and environmental)<sup>178</sup>. These benefits and various regulatory requirements in sectors such as food networks [CSH+ 2014], pharmaceuticals<sup>179</sup>, and clothing<sup>180</sup> have provided a boost to research and development in this

---

<sup>178</sup> [https://www.bsr.org/reports/BSR\\_UNGC\\_Guide\\_to\\_Traceability.pdf](https://www.bsr.org/reports/BSR_UNGC_Guide_to_Traceability.pdf)

<sup>179</sup> <https://www.who.int/medicines/regulation/traceability/7OCT19draft-WHO-policy-brief-on-Traceability-of-Health-Products.pdf>

<sup>180</sup> [https://www.unece.org/fileadmin/DAM/trade/SustainableTextile/2020\\_April\\_Webex/Draft\\_Mapping\\_of\\_Regulations\\_Policies\\_and\\_Guidelines\\_for\\_TT\\_22.04.20.pdf](https://www.unece.org/fileadmin/DAM/trade/SustainableTextile/2020_April_Webex/Draft_Mapping_of_Regulations_Policies_and_Guidelines_for_TT_22.04.20.pdf)

area, and at present there are various processes and tools to effectively and efficiently manage traceability in the supply chain [KLK 2019]. Nevertheless, there are still several challenges to be addressed in order to create such data sharing environments. One challenge is the existence of heterogeneous information management systems and formats, as there are multiple open and de facto standards to support supply and logistics, such as communication standards, syntax definition standards, technical paradigms, and data semantics<sup>181</sup>. Other issues include obtaining critical, accurate, and up-to-date information from other actors, and the overall complexity and cost of integrating traceability systems [KLK 2019].

#### *Electronic Data Interchange Formats.*

In order to facilitate the implementation and deployment of data sharing processes, one approach is to make use of *common technological solutions*. For example, in the business world, EDI (Electronic Data Interchange) infrastructures have been built for quite some time, which facilitate the exchange of business information (e.g. purchasing, forecasts, bidding, billing) between companies [NMH 2009]. Still, EDI requires that the parties agree on the format and content of business information, which leads to fragmentation of the specification and interoperability challenges [Feuerlicht 2011]. As a result, there are other standards that are more focused on providing support for traceability processes, with clearly defined digital identifications and data exchange protocols. One example of this are the GS1 standards<sup>182</sup> that i) allow all actors to identify their assets through globally unique ID keys (e.g. GS1 ID keys), ii) capture this identification information through manual (e.g. barcode) or automatic (e.g. RFID) means, iii) describe the context and events related to this data capture using a Core Business Vocabulary (CBV) standard, and iv) exchange relevant information with other actors through the Electronic Product Code Information Services (EPCIS) standard. The integration of these traceability services brings not only operational benefits but also security and safety benefits: it is possible to implement services that can automatically analyse the available information in the search for potential issues and/or exceptions (e.g. an asset has passed its expiration date, an asset is being stored with other dangerous goods). Moreover, it is also possible to further enhance these standards with the integration of additional technologies, such as the Internet of Things [BHB 2019]. These technologies allow the provision of real-time transparency, as the state and location of assets can now be tracked at all times.

#### *Permissioned Blockchains and Deterministic Smart Contracts.*

Moreover, one particular technology, *permissioned Blockchains*, has the potential to improve the security and usability of existing information-sharing ecosystems [WHH 2020]. A permissioned Blockchain enables the creation of a distributed storage of immutable information where no central organisation needs to manage the transactions, thus facilitating the creation of a federated environment. In such an environment, not only does every member that interacts with the Blockchain need to be authenticated, but it is also possible to provide private information repositories where only a subset of the members is authorised to access the data. Additionally, deterministic smart contracts can be used to define the business logic of supply-chain management applications, enabling the automatic exchange and analysis of supply chain events. As a result, permissioned Blockchains can decrease management and transactional costs, implement automatic analysis mechanisms based on events, support the operations of SMEs, and provide

---

<sup>181</sup> <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=15354>

<sup>182</sup> <https://www.gs1.org/standards/>

environmental benefits [GKH+ 2020]. As of 2021, not only there are several Blockchain-based proofs-of-concept that are being applied to a variety of supply chains (e.g. food, pharmaceuticals, manufacturing) all over the world [GKH+ 2020], but also the number of research articles in this area is growing immensely [MKL 2021]. Moreover, there are also various studies that have analysed the integration of Blockchain with existing data sharing supply chain technologies (e.g. EDI [WLK+ 2017] and EPCIS<sup>183</sup>) and with IoT infrastructures [QTB 2019], although more work is needed in this area [PIE 2021].

#### *Decentralised Identifiers and Self-Sovereign Identities.*

There is still one additional aspect that needs to be carefully considered when sharing information in supply chains: the identity of all partners. Standards such as EPCIS assume that all partners will make use of traditional authentication frameworks, such as PKI X.509, in a federated ecosystem [EPCCert 2010]. Nevertheless, as supply chains are complex and distributed ecosystems, it might be possible to integrate distributed identity concepts such as *Decentralised Identifiers (DIDs) and Self-Sovereign Identities (SSIs)* [MGG 2018]. Here, all actors and entities can have a persistent and globally unique identity that does not depend on any centralised authority, as a proof of this identity is stored within a sufficiently secure decentralised network (e.g. a Blockchain). As of 2021, only a few works explore the applicability of DIDs in supply chains, such as [OB 2020] (smartphone anti-counterfeiting system based on a decentralized IMEI database), [BVH+ 2019] (decentralised peer-to-peer trust marketplace that connects SSI owners with regulatory compliant service providers), and [COC 2021] (digital identity management systems applied to food supply chains).

As aforementioned, even if these technologies bring various security and safety benefits to data sharing infrastructures in supply chains, there are still several challenges facing the application of these technologies. For example, there are various open problems with the adoption of Blockchain solutions for supply chains, including technical limitations (scalability, interoperability, control of off-chain tasks) and issues related to the industry (regulations and policies, standardisation, the link between physical and digital products, and privacy concerns) [SMD+ 2020] [HRK 2019] [MKL 2021]. Moreover, as Blockchain is still a largely unexplored technology, its own security challenges are beginning to be identified and studied, including attacks against the blockchain structure, peer-to-peer system and applications [SSN+ 2020], plus attacks against the authentication infrastructure in permissioned systems [GUG 2021]. Finally, it is necessary to consider that Blockchain is not the silver bullet that will solve all data-sharing issues in supply chains: it is a high-overhead technology that might be more suitable when the level of trust between supply chain partners is low [KLS 2020]. As for the Internet of Things, its (security) challenges and potential security solutions have been already well documented (cf. [RLG 2018] and [ENISA 2018]), although there are still few specific challenges related to its integration in supply chain processes, such as ensuring the validity/integrity of the information acquired by the IoT devices.

#### **4.6.1.4 Monitoring for compliance**

In order to increase trust between supply chain partners, it is essential to have a certain assurance that all processes and services are working as intended and that all products have their advertised features.

---

<sup>183</sup> <http://info.rfid.auburn.edu/chip-proof-of-concept-results>

Compliance with **external certifications** can fulfil this role, as they can reassure all actors that their partners are implementing procedures related to quality, environment, health, safety, and security, among others [WOH+ 2018]. More specifically, there are various security-related standards that can be used by certification bodies as a foundation for the creation of conformity assessment schemes (i.e. certification schemes) in supply chains. For example, the ISO/IEC 27000 series of standards [ISO/IEC27000 2018] provide best practice recommendations on information security management, ranging from generic security requirements and their associated security controls to specific security requirements targeted at particular verticals (e.g. ISO/IEC 27036 and information security for supplier relationships). There are also other standards, such as the ISA/IEC 62443 series of standards<sup>184</sup>, that focus on addressing security vulnerabilities in industrial automation and control systems: ISO/IEC 15408 (“*Common Criteria*”) [ISO/IEC15408-1 2009], which provides formal recognition that a developer’s claims about the security features of their product are valid, and ISO/IEC 20243 (“*O-TTPS*”) [ISO/IEC20243-1 2018], which addresses specific threats to the integrity of hardware and software COTS ICT products. Most of these standards have been approved and implemented as European standards with few or no changes by CEN/CENELEC.

Note that, in Europe, there was a fragmentation of certification schemes across the Member States and sectors, which resulted in a disparity of evaluation methodologies and criteria, and governance rules. As a result, the EU Cybersecurity Act (CSA), established in 2019<sup>185</sup>, defined a framework for security certification. Within such a framework, managed by ENISA, multiple certification schemes will be created for different categories of ICT products, processes and services. ENISA then defined the steps for the definition of new certification schemes (cf. [ENISA 2020D]), which cover the main evaluation areas covered in the assurance framework, including security functional testing, vulnerability testing, robustness testing, and penetration testing. Moreover, ECSO (the European Cyber Security Organization) has pointed out the need to analyse the conditions and procedures required when seeking the certification of products that are composed of assembled certified components (“certification composition”)<sup>186</sup>.

As of 2021, the work on all these areas (development of EU certification schemes, certification composition) is still ongoing. In May 2021, ENISA presented the candidate EU cybersecurity certification scheme, or EUCC scheme<sup>187</sup>, whose role is to succeed the existing schemes operating under the SOG-IS MRA (“Senior Officials Group Information Systems Security” - “Mutual Recognition”) agreement. This EUCC scheme focuses on the certification of ICT products cybersecurity based on the Common Criteria, the Common Methodology for Information Technology Security Evaluation, and corresponding standards such as ISO/IEC 15408 and ISO/IEC 18045.

#### *Limitations of Compliance Certifications.*

However, we have to consider that compliance with security certifications might not guarantee security assurance, which is a known issue described various years ago [DW 2014]. The reason for this is simple. Certification schemes can attest that the processes, services and products of a certain supply chain actor comply with a minimum set of security requirements. However, this compliance is only completely true at

---

<sup>184</sup> <https://www.isa.org/standards-and-publications/isa-standards/>

<sup>185</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0477&from=EN>

<sup>186</sup> <https://ecs-org.eu/documents/uploads/product-composition-document-november-2020.pdf>

<sup>187</sup> <https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1>

the moment when the external audit is performed, plus surveillance audits are usually performed once a year (or less based on scope, risk, and size). Moreover, even if the requirements that involve the deployment of situation awareness procedures are in place, the security environment in which companies operate is very hostile, and an attacker can take advantage of a vulnerability and gain control over some of the actor assets at any time [DW 2014].

### *Continuous Certification.*

One strategy to manage this issue is to change how some of the processes that comprise the certification process are approached: not as evaluations performed at a point in time, but *executed continuously, even in real-time*. By following a “trust, but verify” principle, supply chain actors can assume that their partners already implement various security requirements, yet can check whether some of those requirements still hold true. In fact, the need to provide regular proactive benchmarking of the security measures and policies in the context of supply chains was already identified in 2005 [PPW+ 2005]. Later research [MTA 2010] [NV 2017] also indicated that it was necessary to go beyond the traditional audit model, as the integration of IT technologies would facilitate the implementation and deployment of continuous certification processes.

Although the notion of continuous certification is in its infancy, there are already several studies that explore its applicability, especially in cloud computing ecosystems. For example, the HORIZON project EU-SEC<sup>188</sup> explored the technological requirements that are necessary to implement a continuous auditing-based certification process for cloud services, including the collection, measurement and evaluation of evidence [KB 2019]. Some researchers also used this idea as a foundation in order to define potential architectures that could be applied against the EU Cloud Certification Scheme [ORU 2021]. Going even further, the Security Trust Assurance and Risk (STAR) program, by the Cloud Security Alliance, already provides the STAR Continuous component: a means to facilitate the execution of continuous certification processes<sup>189</sup>. This is done by defining and deploying a set of automated and manual testing processes, which are performed at a certain testing frequency. While these projects do not focus on real-time certification, there are other certification bodies that are exploring, and even applying, this concept. For example, in the IoT ecosystem, certain certification bodies<sup>190</sup> incorporate continuous vulnerability monitoring services into their certification programs, where the security of the IoT products and their ecosystem (mobile applications, back-end infrastructure) are continuously assessed.

In order to provide continuous certification, it is necessary to have various tools that continuously implement the testing procedures indicated in the certification schemes. There are already several approaches that might be useful for this purpose, as their goal is to continuously analyse and validate the security capabilities of different types of devices and infrastructures. For example, in Cloud/Edge computing ecosystems, there are methods that make use of Trusted Platform Module (TPM 2.0) capabilities to evaluate/audit the platform integrity of edge nodes within edge computing ecosystems [AMN+ 2020]. Other approaches focus on IoT

---

<sup>188</sup> <https://www.sec-cert.eu/>

<sup>189</sup> <https://cloudsecurityalliance.org/artifacts/star-continuous-technical-guidance/>

<sup>190</sup> <https://www.intertek.com/cyber-assured/>

technologies, such as the automatic extraction of Manufacturer Usage Descriptors (MUD) through automated IoT security testing methodologies [MRP 2019] [MAZ 2021], or on software development and software operation (DevOps), where the software artefacts produced at each stage of the development process are evaluated according to certain requirements and metrics [AAG+ 2019]. Besides, we have to consider that there are various results in the area of automated vulnerability analysis that focus not only on traditional IT ecosystems, but also on other emerging technologies, such as IoT [YZC+ 2020] and Cloud/Edge applications [KMP+ 2019]. In fact, the notion of automated analysis and management - not only for certification but also for maintenance - has been identified as one of the potential security requirements of future 6G networks [JE 2021].

#### 4.6.1.5 Issues on the Software Supply Chain

The previous state of the art sections mostly focused on the use of information technologies on supply chains that manage physical assets. However, in light of recent events, we also have to consider another dimension of supply chains: the software supply chain, with software elements that also need to be tracked and managed. This is especially important given the use of open-source components in software infrastructures, where 90% of the average codebase is composed of open-source components. However, 29% percent of the top-10 most popular open-source projects contain security vulnerabilities. Moreover, the number of attacks targeting open-source software projects and components is increasing exponentially, growing 450% from July 2019 to May 2020 [Sonatype 2020] and 650% from June 2020 to July 2021 [Sonatype 2021]. Many of these attacks are quite nefarious, as attackers inject vulnerable code in open-source repositories that can be exploited later. As a result, the number of high-profile attacks is increasing steadily, which in turn creates both a huge economic impact and a reduction of trust on the IT infrastructures [Sonatype 2021]. In the last years, these threats caused the creation of new guidelines that aim to provide a set of high-level secure software development practices, including the creation of a Software Bill of Materials (SBOMs) that specifies the list of software used in every device. This area is still in its infancy, with challenges such as the contents of the SBOM, the tools needed to exchange this information [Martin 2020], and the existence of hidden dependencies<sup>191</sup>. However, the explosive growth of software supply chain attacks has kickstarted a global effort to accelerate the implementation of these concepts. Examples of this are the different executive orders and laws signed by countries and unions like the USA, UK and the EU [Sonatype 2021], and the efforts from governments and non-profit organizations like NIST<sup>192</sup>, ENISA<sup>193</sup>, and OWASP<sup>194</sup>. Nevertheless, advances in the research front are still limited, and even if some aspects have been defined in the past years (continuous validation of components through vulnerability analyses, specification software ecosystems where components are tested and validated as a whole [SA 2018]), more work is needed in this area to facilitate the integrity of the software supply chain.

---

<sup>191</sup> <https://cybersecurity.att.com/blogs/security-essentials/software-bill-of-materials-sbom-does-it-work-for-devsecops>

<sup>192</sup> <https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8397.pdf>

<sup>193</sup> <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>

<sup>194</sup> <https://owasp.org/www-project-cyclonedx/>

## 4.6.2 SWOT Analysis



Figure 8: Supply Chain SWOT Summary

In our globalised economy, supply chains are built internationally. The need to secure global supply chains is highlighted by the numerous attacks in the past, as mentioned in the state-of-the-art section (4.6.1) as well as in the major incidents section (4.5). In particular, a recent ENISA report states that “*Supply chain attacks are now expected to multiply by 4 in 2021 compared to last year*”.<sup>195</sup> Those threats are often enabled as a result of greater digitisation of processes and interconnectivity of organisations/companies. In particular, IT providers that are strongly interconnected with their customers’ IT systems are a primary target of attacks. This high interconnectivity makes it easier to inject and spread malware at a large scale, with extensive effects on the supply of society. Moreover, hackers have professionalised, and groups such as Evil and Darkside are meanwhile acting like businesses by offering attacks for sale with extensive support. The increasing acceptance of crypto currency such as Bitcoin is yet another aspect that contributes to the increase in cybersecurity threats. All of this was intensified through an increased attack surface for supply chains

<sup>195</sup> <https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks>

because of the COVID-19 pandemic, which led to more remote working and a likelihood that security safeguards would not be as robust in the home office as in the context of corporate boundaries. As stated in the reports, the impact of cyber-attacks on supply chains has significantly increased, with regard to both the number of incidents and the magnitude of their costs (for recovering from attacks and in particular also for ransom, where the average ransom demand is 5M\$ per case,<sup>196</sup> rather than in the thousands as was the case in the past).

A 2019 report by Huawei<sup>197</sup> points out that risk-based approaches proved to be suitable for addressing cybersecurity threats to supply chains. The author also stresses the need “to participate in industry consortia that help develop standards, and to work with regulatory and governmental bodies” as best practices for tackling the identified threats and risks. Hence, supply chain security is a global concern and must be addressed globally and in a coordinated fashion. A SWOT (Strength, Weakness, Opportunity, and Threat) analysis is conducted to understand the EU’s preparedness to tackle the threats arising from supply chain attacks, becoming an enabler, and if possible a leader, in this field by eliminating the weaknesses and taking advantage of the current opportunities. Detailed SWOT analysis results are presented below.

#### 4.6.2.1 Strengths

- The EU’s **financial and economic power** make the Union a major player in the world, both, with regard to producers and consumers of goods: Europe could define security standards in the industries and sectors in which it plays a leading role and eventually lead to a global spread. EU consumers have the power to change products, e.g. how they are produced, for instance with regard to reduced greenhouse gas emissions, energy efficiency, or the right to repair that impacts a reliable supply chain. Therefore, the EU has the strength to demand a transparent supply chain for products that are produced or sold in EU countries.
- The EU has a high standard of education, and European companies and academia show **high design and engineering knowhow** and are strong in developing technical solutions e.g. engineering, design, and research.
- For example, with the Horizon 2020 initiative, the EU offers substantial **research funding** of almost €80 billion to ensure Europe’s competitiveness. Concerning supply chain security, the EU and its partner countries have become aware of security challenges through supply chain attacks in the past and have created and funded projects to react and be prepared in this regard, e.g. Customs Detection Technology Project Group (CDTPG), SecureSCM, Cybersec4Europe, etc. In total, the EU has produced over 2000 project deliverables and publications in the supply chain domain.
- The economy of the EU **is a leader in certain key industries**. This means that, in sectors of the economy where EU companies play a leading role, such as machinery and automotive, these companies can enforce supply chain security requirements for their domains.
- The EU’s ENISA has created a comprehensive set of **European security recommendations and guidelines** for combating supply chain attacks, such as focusing on supply chain integrity [ENISA 2015], healthcare and Industry 4.0 [ENISA 2019A], and for secure ICT procurement of electronic communications [ENISA 2014].

<sup>196</sup> <https://www.paloaltonetworks.com/blog/2021/08/ransomware-crisis/>

<sup>197</sup> [https://www-file.huawei.com/-/media/corporate/pdf/public-policy/huaweis\\_position\\_paper\\_on\\_cybersecurity.pdf](https://www-file.huawei.com/-/media/corporate/pdf/public-policy/huaweis_position_paper_on_cybersecurity.pdf)

- Many EU organisations and companies are part of the Open Trusted Technology Forum (OTTF), whose aim is to increase product integrity and supply chain security by developing **open standards and certification programs**.

#### 4.6.2.2 Weaknesses

- The EU **lacks leadership in important economic sectors, such as consumer electronics, IT and software**, with some exceptions in industrial domains such as automotive: “The EU’s tech industry is lagging behind these Silicon Valley giants” [Schäfer 2018]. Hence, driving innovations in these sectors and defining standards that others will follow is a challenging task.
- In today’s globalised world, supply chains do not follow national borders, but **depend on global, highly distributed, and complex supply chain networks**. The EU imports or uses many hardware and software products manufactured and developed in other continents, in particular the Americas and Asia; therefore, the EU is dependent on global supply chains.
- As of today, there is no EU-wide catalogue of measures that uniformly regulates the security of supply chains, e.g. as GDPR does for privacy concerns. Hence, because of **missing supply chain security standards**, the security compliance of supply chains is currently hard to enforce.

#### 4.6.2.3 Opportunities

Currently, suppliers may use their own process and may not adhere to a common regulation. In this scenario, traceability becomes difficult and one faces difficulties in finding the information necessary to validate the integrity of the supply chain.

The opportunities that the EU has are the following:

- The strong technical expertise of the EU enables it to do the product design and engineering in house and, finally, secure supply chains allow the **validation of the integrity of the final product** which could be produced and integrated in different continents. With EU companies having secure supply chains and thereby being able to control and validate compliance, they are also able to better monitor the reliability of their suppliers. That also allows them to provide transparency and to gain the customer’s trust in the quality of their products.
- The EU can initiate coordinated actions and **introduce supply chain security standards** and regulations to compel organisations to comply with supply chain security measures and to protect the EU’s sovereignty, e.g. similarly to GDPR. For example, a supply chain integrity (SCI) regulation could be defined, requiring manufacturers to use common and standardised data exchange formats (such as eCI@ss<sup>198</sup>) that include sufficient information to validate the integrity of the supply chain.
- Overall, the EU follows a cooperative globalisation approach and, hence, is in a good position to **support and promote a global approach** to supply chain security. A recent report<sup>199</sup> mentions that independent reviews and audits of products are needed for regaining trust in the world’s supply chain. This is important, because manufacturers do not want to reveal trade secrets, but on the other

<sup>198</sup> <https://www.eclass.eu/>

<sup>199</sup> [https://www-file.huawei.com/-/media/corp/facts/pdf/2019/huawei-white-paper\\_tony-scott\\_final.pdf?la=en](https://www-file.huawei.com/-/media/corp/facts/pdf/2019/huawei-white-paper_tony-scott_final.pdf?la=en)

hand, consumers and product owners need to know the origin and qualities of goods consumed (e.g. to be sure that they have not been produced via child labour).

- As trust in product quality is a major motivating factor for customers to buy goods, **secure supply chains contribute to strengthening the economy**. The EU's economy would benefit from increases in productivity, trust, and sales if supply chains were more reliable, transparent, and tighter integrated. The EU has the opportunity to launch new and/or to support existing initiatives that focus on securing supply chains in certain sectors or across sectors.
- An aspect relevant with respect to supply chains is being able to ascertain the **carbon footprint** of the goods involved. There are initiatives that aim to contribute to the reduction of that footprint. For instance, the non-profit association ESTAINIUM<sup>200</sup> focuses on decarbonising industries “by providing access to digital technologies that demonstrate scientifically sound ways of identifying, reporting, documenting and compensating for climate-negative impacts”. Technologies such as blockchain, decentralised identifiers (DID) and verifiable credentials (VC) which are also investigated by CyberSec4Europe can contribute significantly to make this information available within supply chains in a reliable and verifiable manner. This infrastructure can then be used to communicate and use such data by individual industrial players that already started concrete developments in this direction - so did Siemens that is a partner in CyberSec4Europe with SiGREEN<sup>201</sup>. Such ventures can lead to strong competitive advantages for European companies in certain sectors as global suppliers become more integrated.

#### 4.6.2.4 Threats

- **EU companies may resist the adoption of new supply chain regulations** if proposed by the EU or a global organisation, because of bureaucratic expenditure they fear. The introduction of corresponding regulations might be hindered through lobbying.
- **Reduction of research funds:** Future research and funding for a secure supply chain could be affected because of prioritised events or crises like the COVID-19 pandemic.
- **High innovation cost:** A lack of economic growth during crises such as the COVID-19 pandemic could negatively affect EU supply chains and the willingness of companies to invest in new supply chain management technologies, because of costs and high risks that it might fail or might not be adopted by other players in the world.
- **Increased complexity & bureaucracy:** To adopt and use any new regulations, e.g. to properly enforce regulations such as GDPR, a great deal of effort is required
- **International/political resistance** to adopt new standards or regulations, because each country and organisation wants to enforce their own policies and standards.
- In the case of lack of progress and development, other firms/trading partners could move much faster and the EU would need to adopt the rules of more dominant partners like the USA and China, i.e. agreements without the EU being part of it. That is, the **EU would miss the opportunity to become the leader in this initiative**.

<sup>200</sup> <https://profiles.eco/estainium>

<sup>201</sup> <https://www.siemens.com/sigreen>

### 4.6.3 European Digital Sovereignty

For the EU, the goal of achieving a “digital supply chain” has been pursued for some time. For example, the European Commission launched the eBiz TCF action (integrating 17 pilot projects with more than 150 companies from 20 European countries) to help SMEs to participate in global digital supply chains in the textile and clothing sectors in 2008. Moreover, in the “New Industrial Strategy for Europe” (published in March 2020), the EU stated that the benefits of digital supply chains can accelerate the implementation of several strategic objectives, which will facilitate a globally competitive and world-leading European industry. Such strategic objectives include the identification of supply chain dependencies, the secure supply of clean and affordable energy and raw materials, and ensuring balanced responsibilities for all market players depending on their position in the supply chain. Therefore, it is clear that the EU considers the digital supply chain as a part of main initiatives in the future.

However, not only the current climate of hostile threats and attacks that target supply chain ecosystems, but also the COVID-19 pandemic, has shown us that the security (and resilience) of supply chains is crucial to any kind of sovereignty. In terms of supply chains in digital markets, the issue is at least double-faced, in that “security of a supply chain” means that all required items can be supplied when needed, but also that all items that are indeed supplied are individually exempt from security concerns. Therefore, it is crucial to strengthen the security of EU supply chain actors and processes on all fronts (from technology to standardisation) so as to adequately respond to these challenges.

Research into supply chain security will contribute to this concern by providing solutions to these interdisciplinary challenges. For example, as mentioned above, within the complex interconnected web of supply chain networks there is a layer of OT and IT systems, which include cutting-edge systems such as the cloud and the Internet of Things. Such a layer needs to be continuously protected, as both external and internal attackers could manipulate these systems for various purposes (such as sabotage and industrial espionage). Another challenge is related to the security and privacy of the information assets and goods: as supply chain ecosystems are complex and intertwined, it becomes essential to develop privacy-aware data-sharing infrastructures, where multiple parties can share information about assets, goods, and supply chain processes and events in a secure and private way. This will facilitate the automatic analysis of supply chain workflows, and the discovery of exceptions and anomalies. Last but not least, it is important to recall the dual nature of existing supply chains, where the goods that are managed and processed within the supply chain can be either physical or digital. Therefore, not only for the manufacturing of physical goods, but for the development of software solutions as well, it is necessary to ensure that both suppliers and raw materials (including software materials such as components and libraries) are continuously monitored for compliance through accreditations and/or by continuous testing.

### 4.6.4 COVID-19 and Public Health Dimension

The COVID-19 pandemic, together with the related safety guidelines and mandated lockdowns, has had a significant impact on the supply chains and whole-value chains that power the global economy. Supply chains are primarily designed with cost and efficiency in mind, often without considering redundancies, reserve stocks, where suppliers get their supplies, etc. All of these considerations could cause an obstacle to continuous supply during the pandemic. The COVID-19 health crisis has exacerbated the problems by also bringing large changes to the balance between supply and demand. Demand for things like personal

protective equipment and toilet paper has risen sharply, while the demand for cars and office supplies has fallen dramatically. At the same time, the supply was affected by the sharp fall in production, as a direct result of the virus (sick workers), national/regional policies for reducing the spread of the disease (blocked transport routes and factory shutdowns or limited production), and/or by any of the previous reasons further down the supply chain, limiting their output and in turn all consequent production in the supply chain.

The wide scope of the effects on supply chains caused by the COVID-19 pandemic is also shown by the McKinsey survey of global Supply Chain leaders (performed in May 2020),<sup>202</sup> where 73% of the participants encountered problems in their supply and 75% of them had problems in production and distribution as a result of the COVID-19 crisis. Almost half of the respondents reported a slowing down of decision-making in planning due to working from home, while 85% of the participating organisations reported problems as a result of inefficient digital technologies in their supply chains. They stressed the importance of having good control over supply-chain technology in an organisation, and nine out of ten surveyed organisations are also planning to increase the amount of digital supply-chain talent within their organisations. As a result, COVID-19 seems to have primarily sped up the processes already underway before the crisis. Primarily, this includes regionalisation of trade and production networks, the growing role of digitisation, the focus on proximity to consumers and the increased use of automation technologies in manufacturing.<sup>203</sup> While automation can offer more resilience in the face of pandemics and other situations that prevent people from working, it can also entail higher vulnerability to cyberattacks.

In addition to easier and more efficient management, digitalisation of supply chains can also bring other benefits to organisations, especially in extreme situations like the pandemic. The Nike<sup>204</sup> company has used their advanced supply chain management capabilities to reroute the goods heading to brick-and-mortar stores to an online retailers/distribution warehouse, after it became apparent that shopping in person would become difficult or even impossible, depending on local restrictions. The goods were, therefore, already in the appropriate location when the switch from shopping in person to predominately online shopping happened. The high level of information gained from their supply chain solution also enabled the company to recognise which of their existing and/or upcoming products were running low in stock at a time when producing new items was not feasible, as a result of the changes and limitations brought about by the COVID-19 crisis. They used this information to steer their marketing campaigns to promote products that were still readily available and/or were being produced without a problem.

An interesting aspect of managing a supply chain under the COVID-19 circumstances is also one of managing human resources, in particular those concerned with the transport of goods. Goods (especially essential and emergency supplies) have to be transported and therefore, even during the lockdown, transportation of goods was to some extent excluded from these limitations. People who deliver can spread

---

<sup>202</sup><https://www.mckinsey.com/business-functions/operations/our-insights/resetting-supply-chains-for-the-next-normal>

<sup>203</sup><https://www.mckinsey.com/~media/McKinsey/Business%20Functions/Operations/Our%20Insights/Risk%20resilience%20and%20rebalancing%20in%20global%20value%20chains/Risk-resilience-and-rebalancing-in-global-value-chains-exec-summary-vF.pdf>

<sup>204</sup><https://www.mckinsey.com/business-functions/operations/our-insights/covid-19-and-supply-chain-recovery-planning-for-the-future>

the disease between communities. It is therefore essential to track their movements and possible signs of sickness while maintaining their privacy.

The COVID-19 crisis has also directly impacted the security of supply chains.<sup>205</sup> Many organisations were left with limited or no access to certain suppliers, causing them to have to find substitutions quickly. This caused an increased risk of introducing malicious or at least poorly protected partners into their supply chain. In a hurry to maintain the new supply chains, their cybersecurity might have taken a back seat, and this could result in future attacks. An additional significant contributor to an increased level of risk is the sudden switch to working from home. This increases the attack surface for the attackers, by enabling them to exploit and use equipment and infrastructure not directly under the control of the organisation. This can be especially problematic in environments where remote work was not common beforehand: the new security measures put in place could not be exhaustively tested, and employees who had never worked from home before had to get educated hastily on how to do it securely.

Not only have the emergency conditions facilitated the possibilities of more vulnerabilities being opened in the supply chain systems, but there have also been specific attacks on organisations tasked with regulating and shipping cargo around the world. Two recent examples are the attacks on the shipping company CMA CGM<sup>206</sup> and the International Maritime Organization.<sup>207</sup> The cybercriminals have also exploited the strong public demand for updates on the constantly evolving global health situation by using it as a phishing lure. Multiple COVID-19 malware and phishing campaigns have been detected impersonating, among others, FedEx, DHL and UPS.<sup>208</sup>

The supply chain field has always been important for the public health dimension, but the COVID-19 pandemic has made it more obvious how important the timely supply of drugs, biological products, personal protective equipment and medical devices (including diagnostic and testing devices) is for the health and wellbeing of the general population. As a consequence, the COVID-19 pandemic has also sparked the development of public health supply chain resilience strategies like the Pharmaceutical strategy for Europe<sup>209</sup> or the National Strategy for Resilient Public Health Supply Chain established in the US.<sup>210</sup> They, at least in part, lay down plans for enhancing resilience, diversifying and securing supply chains, crisis preparedness and response mechanisms.

The problem of resiliency is closely related to the challenge of data visibility because, without quick access to dispersed data sources, it is difficult to determine current and future needs, and current stock (across all storage places). Data visibility, therefore, provides the ability to better manage the stock, it can help prevent

---

<sup>205</sup> <https://www.sme.org/technologies/articles/2020/august/ul-says-covid-19-increases-cybersecurity-problems/>

<sup>206</sup> <https://www.supplychaindive.com/news/cma-cgm-ocean-shipping-malware-cyber-attack-information-technology/585978/>

<sup>207</sup> <https://gcaptain.com/international-maritime-organization-hit-by-cyber-attack/>

<sup>208</sup> <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/COVID-19/Deloitte-Global-Cyber-COVID-19-Executive-Briefing-Issue-5-release-date-5.6.2020.pdf>

<sup>209</sup> [https://ec.europa.eu/health/sites/default/files/human-use/docs/pharma-strategy\\_report\\_en.pdf](https://ec.europa.eu/health/sites/default/files/human-use/docs/pharma-strategy_report_en.pdf)

<sup>210</sup> <https://www.phe.gov/Preparedness/legal/Documents/National-Strategy-for-Resilient-Public-Health-Supply-Chain.pdf>

expiration of the medical goods or other waste, it can reduce operational costs, and it improves service levels by optimising processes such as procurement planning and inventory management. However, achieving visibility in supply chains has been a challenge for governments (especially in less developed countries) because of the fragmented (possibly even paper-based) supply chains. Challenges with health supply chains are additionally exacerbated because they are global, multi-tiered, and required to meet stringent regulations. Digitalisation is a way to drastically improve data visibility. This, however, brings with it a strong need for cybersecurity. A connected issue is also the problem of drug counterfeiting, which can also be fought with tracking abilities brought into the system by digitalisation.

#### 4.6.5 Green Deal and Climate Change

With the European Green Deal,<sup>211</sup> the EU has drafted an ambitious roadmap that includes legislative changes and defines the roles and responsibilities of public and private actors to protect the environment and ecosystems worldwide, and to fight climate change. While supply chains are not at the forefront of this initiative, they can contribute to it.

The Alliance for Corporate Transparency published a report<sup>212</sup> in 2019 that analysed the sustainability reports of 1000 companies pursuant to the EU Non-Financial Reporting Directive. The analysis included the environmental and societal risks and impacts disclosed by the companies. The report (among other things) found that supply chain transparency is low. Less than 1% of the organisations have publicly listed their supplier, and high-risk sectors have not performed any better. The best in this regard is the apparel sector, where 36% give a broad description of the location of their supply chains and 14% list their actual suppliers. Organisations report more on their greenhouse gas emissions, but the numbers are still fairly low. More than two-thirds of companies provide specific key performance indicators for direct emissions, but just barely half report on emissions with energy use taken into account, and just over one third when applied to the company's entire value chain.

In a related issue, a Study on Due Diligence Requirements Through the Supply Chain<sup>213</sup> requested by the European Commission and published in 2020 has found that most businesses surveyed do not systematically address environmental or social impacts in their operations or supply chains. The primary goal of the analysis was to determine options for the EU to standardise risk management of due diligence in companies' operations and through their supply chains, for the benefit of the environment and human rights. Due diligence allows companies and consumers to assure that companies' operations and their suppliers use sustainable and friendly practices towards their employees and the environment.

Research results provided by the CyberSec4Europe project address these requirements by providing support for tracking products in the context of distributed, cross-organisational supply chains. This tracking denotes in particular the tracking of their costs, their origin and location, as well as their environmental impact (e.g. greenhouse gas emissions), data that are necessary to show a company's due diligence. As highlighted in

---

<sup>211</sup> <https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal>

<sup>212</sup> [https://allianceforcorporatetransparency.org/assets/2019\\_Research\\_Report%20Alliance for Corporate Transparency-7d9802a0c18c9f13017d686481bd2d6c6886fea6d9e9c7a5c3cfafea8a48b1c7.pdf](https://allianceforcorporatetransparency.org/assets/2019_Research_Report%20Alliance%20for%20Corporate%20Transparency-7d9802a0c18c9f13017d686481bd2d6c6886fea6d9e9c7a5c3cfafea8a48b1c7.pdf)

<sup>213</sup> <https://op.europa.eu/en/publication-detail/-/publication/8ba0a8fd-4c83-11ea-b8b7-01aa75ed71a1>

the opportunities category of the SWOT Analysis section above, initiatives like ESTANIUM<sup>214</sup> focus on the tracking of carbon emission of, e.g. manufacturing and transportation steps. This contributes to gaining transparency and hence allows the comparison of products, not only in terms of price and quality, but also by their environmental impact. Overall, better traceability of goods also helps to improve the trustworthiness of companies and customers' trust in the products and services provided. CyberSec4Europe contributes to these developments by introducing and evaluating novel approaches for tracking and tracing activities in supply chains in a blockchain-based extensible infrastructure. Using a distributed ledger-like blockchain as underlying technology enables transparency about the origin and processing of products, helping, for example, to evaluate the possibility whether child labour was applied. It can also be used to support the above-mentioned use case of tracking carbon emissions, supporting the exchange of carbon footprint information of products by accumulating the carbon footprint of suppliers' goods, the routes of transportation used and the energy consumed for producing products.

The use of blockchain technology is also often associated with high energy requirements. This is a consequence of, among other things, the high-power consumption of examples such as Bitcoin mining. However, unlike in the case of cryptocurrencies, permissioned blockchains such as Hyperledger Fabric are used in the scenarios mentioned above and also in the context of CyberSec4Europe. Instead of costly consensus operations that depend on proof-of-work, permissioned blockchains used for industrial use cases typically make use of protocols such as proof-of-stake or proof-of-authority, which are far more efficient and thus environmentally friendly [BADA 2021].

Climate change can have a significant negative impact on supply chains, and in the future, risks associated with climate change (e.g. extreme weather conditions) will have to be considered in order to ensure resilient supply chains. Unfortunately, the reverse is also true – the manufacturing and transportation of goods has a significant negative impact on climate change. Supply chains all over the globe are a considerable contributor to greenhouse gas emissions, which is the leading cause of climate change. Supply chains primarily create CO<sub>2</sub> along the manufacturing process, in transportation, and during storage and distribution. However, the modern way of life cannot continue without supply chains; therefore, we have to find ways to reduce the impact they have on the environment.

Digitalisation and data visibility can greatly contribute here by optimising supply chains and eliminating waste. Solutions like the one produced in this project, and already mentioned in the Green Dimension, using a distributed ledger-like blockchain as the underlying technology to ensure transparency of the carbon footprint of goods, can be used in regulations to ensure companies are doing their part to help reduce the emissions, but also by the end consumers to help them choose products that have a smaller impact on the environment.

Likewise, the new technologies based on modelling and simulation supported by preventive measures, such as the digital twin, can also be highlighted at this point by favouring predictive maintenance tasks, and possible uncontrolled emissions that may have a serious impact on the good quality of the environment. But

---

<sup>214</sup> <https://press.siemens.com/global/en/pressrelease/siemens-has-developed-ecosystem-based-approach-exchange-emission-data>

beyond improving the risk management of a system, digital twins can also be efficient ways to contribute to online cyber defence. They could anticipate security risks, detect and locate attacks, and respond in time to avoid major consequences in the context and its environment (e.g. opening of actuators that control chemical products). In this sense, General Electric associates the capacities of the digital twin with the Digital Ghost paradigm.<sup>215</sup> This paradigm focuses on securing industrial assets and critical infrastructure, including its own supply chain, from (deliberate or casual) threats that can put the entire value chain at risk.

Finally, we also have to consider that agile supply chains with good data visibility are also in a better position to help relieve and supply goods to areas stricken by events caused by climate change (e.g. food and water to places suffering from drought or food, and building materials to places struck by tornados).

#### **4.6.6 Impact on Democracy**

Supply chains do not have a direct impact on democracy itself, but severe instability or complete collapse on a larger scale in the supply of basic necessities (e.g. food, medicine, etc.) can very quickly lead to mistrust of the government, panic buying, or possibly rioting and worse. Like many problems with supply chains, this one can also be alleviated by digitalisation; and as we have discussed in the public health section, digitalisation brings the power to better manage, predict and plan the distribution and procurement of goods, which helps to prevent any such large-scale supply chain collapse from happening.

#### **4.6.7 Contributions to the EU CyberSecurity Strategy for the Digital Decade**

The EU's Cybersecurity Strategy for the Digital Decade<sup>216</sup> is fully aware that critical infrastructures and essential services are increasingly interdependent and digitised, and must be resilient and secure, preferably by design. The EU aims to **lead** in the development of secure technologies across the whole supply chain. Here is exactly where CyberSec4Europe contributes substantially.

##### **4.6.7.1 Resilient infrastructure and critical services**

The EU targets consistent security and incident reporting requirements, including national supervision, and enforcement. Its forthcoming new Network and Information Systems (NIS) Directive will cover strategically important sectors, including energy, finance, transport, navigation and health, and will focus on the resilience of critical infrastructure.

The EU's Strategy explicitly mentions "supply chains for energy technologies being important for the continuity of essential (cross-border) services and for the strategic control of critical energy infrastructure". Regarding supply chains, CyberSec4Europe greatly improves security and the means to audit and enforce compliance, with its use cases addressing critical infrastructures mentioned by the EU's Strategy.

Further developments in the supply chain security technologies addressed by CyberSec4Europe will render supply chains more secure, compliant, and transparent. They can provide the consistency, supervision, and enforcement envisaged by the EU's Strategy, and, with continued support, will enable it to ascertain the desired leading position.

---

<sup>215</sup> <https://www.ge.com/research/offering/digital-ghost-real-time-active-cyber-defense>

<sup>216</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=EN>

#### **4.6.7.2 Building a European Cyber Shield**

The EU's Strategy targets the establishment and strengthening of information and analysis sharing in Security Operations Centres (SOCs) through their respective Security Information and Event Management (SIEMs). Basically, the main goal of these SOCs is to allow multiple stakeholders to cooperate to combat cyber threats and to perform the required constant monitoring and analysis to detect intrusions and anomalies in real time. As we in CyberSec4Europe know very well from our own use-cases, this requires support by AI-based techniques and machine learning; both are technologies we can apply and improve successfully to secure supply chains.

The SOC network to be set up by the EU can profit from the AI technologies developed by CyberSec4Europe. In the context of the EU's funding SOC network establishment a transfer might be possible, and we can contribute to make information sharing more secure, confidential, traceable and effective. In turn, support by this SOC network will be beneficial for supply chain security, by enabling a fuller situational awareness, more timely warnings and sharing of best practices.

#### **4.6.7.3 An ultra-secure communication infrastructure**

The satellite- and terrestrial-fibre-based secure quantum communication infrastructure, which is part of the EU's Strategy, currently focuses on the security- and safety-critical missions and operations of public authorities and critical governmental activities. Supply chains might also benefit from such a communication infrastructure.

Vital prerequisites for the establishment of such a secure communication infrastructure are highly secure supply chains, where every component can be traced reliably and its origins and quality can be determined with confidence. The EU's Strategy explicitly stresses preference for European technology and the fundamental need for ascertaining compliance. CyberSec4Europe can meet this need with its technologies, securing Europe's cutting-edge ultra-secure communication infrastructure.

#### **4.6.7.4 Securing the next generation of broadband mobile networks**

Applications enabled by 5G and beyond should, according to the EU's Strategy, excel in security protected by EU measures. Improving the security of mobile networks with new technologies is not within the focus of CyberSec4Europe. However, for this building up the underlying mobile network infrastructure must avoid dependencies and be supported by a secure sustainable and diverse supply chain. As with the governmental communication infrastructure referred to in the previous section, it is vital that all parts can be traced as they pass through the supply chain and that their provenance and quality are assured. CyberSec4Europe's technologies and approaches enable this, reduce the need for hierarchical trust, and support the EU's Strategy by minimising the exposure to and dependence on high risk suppliers.

#### **4.6.7.5 An Internet of Secure Things**

IoT users face the risk of being exposed to insecure connected things, as the EU is well aware. Essential prerequisites to safeguard against insecure products and services are secure and transparent supply chains and the ability to enforce compliance on suppliers and supplied goods, in addition to being able to trace items and their quality, all of which we support in CyberSec4Europe. The certification scheme envisaged by the EU's Strategy depends on such capabilities.

#### **4.6.7.6 Greater global Internet security**

The domain name system (DNS) is at the core of the Internet, but its security is not adequate for its vital and central importance. Unavailability of the Internet would be detrimental not only to supply chains. The EU's strategy is to plan for business continuity if the DNS were affected adversely, and to improve monitoring and sharing of information, and advice on potential disruptions. Among other things, there should be secure public DNS resolvers operated by EU entities. The EU's Strategy is to encourage relevant stakeholders to adopt a DNS resolution diversification strategy. CyberSec4Europe is not targeting improvements, but would greatly welcome such enhanced Internet security and reliability for the sake of supply chains.

#### **4.6.7.7 A reinforced presence in the technology supply chain**

This particular aspect of the EU CyberSecurity Strategy focuses mostly on i) propelling *EU strategies and leadership in technologies and cybersecurity* across the digital supply chain, and ii) seeking a key role in developing the *EU's sovereignty* in cybersecurity: that is, securing sensitive infrastructures and reducing dependencies in other parts of the globe for these infrastructures. Regarding the first aspect, in order to achieve leadership across the digital supply chain we also need to consider the supply chains themselves. As shown in this roadmap, without the means to enforce compliance, we will have no control over the integrity of our technologies. It is then essential that Europe should take the lead in the development of supply chain security standardisation efforts that respect European values.

As for the second aspect, we have already discussed in section 4.6.3 that research into supply chain security will provide solutions to several interdisciplinary challenges crucial to our sovereignty, such as the identification of supply chain (security) dependencies, and ensuring balanced responsibilities among all actors in the supply chain. Some of these solutions are already being explored in CyberSec4Europe, such as traceability in workflows. All of this will facilitate a robust and secure supply chain, which will allow us to build our European infrastructures (e.g. 5G infrastructure) with a higher degree of trust.

#### **4.6.7.8 A Cyber-skilled EU workforce**

While research in this vertical does not directly contribute to the development and attraction of cyber-skilled talent, the cutting-edge nature of several of the challenges described by CyberSec4Europe in this roadmap will increase their appeal. This, in turn, will pull talented professionals into this area - provided they are offered the necessary incentives. In addition, some technologies that could be used to solve these challenges, such as Digital Twins (to enhance, for example, Cyber-Range models [VIE 2021]), can also be applied to facilitate education/training in a number of cybersecurity-related areas, such as the analysis of anomalies, as they allow students, future experts on cybersecurity or employees to test various tools in a realistic environment without a physical infrastructure. Therefore, further developments in these technologies will also lead to an improvement in cybersecurity education.

#### **4.6.7.9 EU leadership on standards, norms and frameworks in cyberspace**

As discussed during this roadmap, there are various standards and norms in the area of supply chains and supply chain cybersecurity that need to be defined and/or enforced. More specifically, the knowhow obtained from the development of the challenges in this vertical can be used as a foundation to develop these standards and norms. Moreover, as shown in the SWOT analysis presented in section 4.6.2, the EU should initiate coordinated actions and introduce supply chain security standards and regulations to compel

organisations to comply with supply chain security measures. In fact, the EU is in a good position to support and promote a global approach to supply chain security.

#### **4.6.7.10 Cooperation with partners and the multi-stakeholder community**

Supply chain security is a global concern; thus, it must be addressed globally and in a coordinated fashion. Therefore, while researching and providing solutions to the challenges described and highlighted in this vertical by CyberSec4Europe, EU actors will collaborate and cooperate with various entities in third countries, from research institutes to organisations and governmental bodies. This is an opportunity to fulfil several goals highlighted in the cybersecurity strategy, such as promoting the EU values and vision, exchanging information and coordinating on developments in this area, and reinforcing regular and structured exchanges with all stakeholders.

#### **4.6.7.11 Strengthening global capacities to increase global resilience**

The contributions of this vertical described in the previous sections 4.6.8.9 and 4.6.8.10, namely the development of supply chain security standards and regulations plus the collaboration with third countries, are also applicable to this initiative. As such standards and regulations have a global reach, they will be deployed in partner countries, resulting in trustworthy supply chain infrastructures that include cybersecurity as a standard feature. This will strengthen such countries against malicious cyber activities, reducing the impact of cyberattacks that could undermine their economic and political stability.

### **4.6.8 Sector-specific Dimensions**

The supply chain vertical is closely related to other verticals due to its inherent heterogeneity and complexity, and as such it is essential to consider its interactions with other verticals and its dimensions - especially privacy-preserving identity management (for the identity of all actors in the supply chain ecosystem), incident reporting (for the management of threat intelligence between supply chain partners), and maritime transport (as maritime transport is one of the backbones of supply chains).

#### **4.6.9 Summary of the dimensions and impact on the Roadmap**

As we have mentioned, there are various aspects, or dimensions, that we have to consider when protecting global supply chains, either physical or digital. Some of these dimensions have shown various weaknesses in this vertical that must be carefully taken into account. Consider, for example, the COVID-19 and public health dimensions. Not only has the pandemic uncovered various underlying issues with existing supply chain strategies, such as the just-in-time management strategy, but it has also highlighted the need to have better tools to improve the overall visibility and resilience of supply chains in a dynamic scenario, where new suppliers are integrated when necessary. However, we have discussed how bringing new suppliers increased both the attack surface and the risk of future cyberattacks; thus, it is necessary to adequately protect such tools. The pandemic has also shown how the digitalisation of supply chains has been accelerated, bringing additional benefits to organisations, such as rerouting goods to where they are needed (e.g. online distribution warehouses instead of brick-and-mortar stores). Still, this sudden digitalisation also brought new attacks, related not only to employees working from their home, but also to more vulnerabilities being opened in the supply chain systems. Therefore, the detection of risks and hardening of infrastructures must not be neglected.

Other dimensions, like the green and climate change dimensions, have shown how the digitalisation of supply chains can contribute to the EU roadmaps that focus on protecting the environment and ecosystems worldwide. By providing support for tracking products in the context of distributed, cross-organisational supply chains, it is also possible to trace the environmental impact of such processes. Such digitalisation and data visibility, including the use of digital twins, can be used to optimise the supply chain processes, eliminating waste and reducing uncontrolled emissions. This digitalisation can make use of efficient blockchain technologies, with consensus mechanisms such as proof-of-stake or proof-of-authority that are far more efficient and environmentally friendly than proof-of-work. Still, if technologies like blockchain are to be used, that means it is necessary to carefully consider the security and privacy implications of such technologies.

Finally, we have discussed how the security (and resilience) of supply chains is crucial to our sovereignty and our democracy. More precisely, we have described how the security of supply chains aligns with the EU CyberSecurity Strategy for the Digital Decade in various aspects. Without i) the continuous protection of the interconnected web of supply chain IT and OT infrastructures, ii) the security and privacy of the information assets and goods shared between partners, and iii) the monitoring and testing of physical goods and software materials, the EU's position as a globally competitive and world-leading industry will be in danger.

Taking account of all the factors described above, we need to consider the challenges described in the next sections in order to provide adequate protection to our supply chains, using mechanisms and services that are proactive and dynamic enough to adapt to our changing world:

- Challenge 1: Detection and management of supply chain security risks.
- Challenge 2: Security hardening of supply chain infrastructures, including cyber and physical systems.
- Challenge 3: Security and privacy of supply chain information assets and goods.
- Challenge 4: Management of the certification of supply partners.

#### 4.6.10 Challenge 1: Detection and management of supply chain security risks

Most supply chain recommendations and standards have focused on the detection and classification of potential supply chain risks, including security risks. Note that the scope of these “security risks” in this context is very broad, as it considers all previously introduced assets: from the fixed/mobile infrastructure to other tangible and intangible assets, including all goods and the IT/OT infrastructure. Managing these risks is a very daunting task, not only because the scope of a security risk is broad in this context, but also because the supply chain ecosystem is very complex and dynamic.

##### Specific Research Goals:

- ***Design evidence-based and context-based risk assessment approaches.*** As stated in Section 8.4.1, this process should be subject to recent cybersecurity incidents and sophisticated attacks (e.g. APT10, APT40, APT27, APT15), as well as on the scenario and its real context. At this level, it is still fundamental to incorporate novel and lightweight learning measures and mechanisms that help identify classes of vulnerabilities (e.g. zero-days in IT/OT assets), compute attack costs (modus

operandi, kind of threat/cyber-attacks, attacker's capacities, etc.) and determine consequences ((inter-)dependencies and impact) to derive new vulnerabilities, attack paths and lateral movements.

- ***Automate IT-OT assets to reactive risk assessment according to the situation*** by monitoring the current and new IT/OT components, their relationships (IT-OT) and their inter-dependencies. Through this process, the risk management engines could update their risk/impact likelihood matrices taking into account complex conditions of the context and its implicit dynamicity.
- ***Trace and visualize attack paths and the flow of the possible attacks in optimal times***. The heterogeneity of the new Supply Chain scenario encourages the incorporation of new context-based traceability measures together with learning mechanisms to estimate and visualize possible/probable collateral movements, forecasting and visualizing possible/probable cascading effects on IT-OT infrastructure.

### JRC Cybersecurity Domain:

- Security Management and Governance
  - Risk management;
  - Threats and vulnerabilities modelling;
  - Attack modelling and countermeasures;
  - Standards for Information Security.

### JRC Sectorial Dimensions:

- Energy;
- Health;
- Maritime;
- Transportation;
- Supply Chain;

### JRC Applications and Technologies Dimensions:

- Artificial intelligence;
- Big Data;
- Blockchain and Distributed Ledger Technology (DLT);
- Cloud and Virtualisation;
- Embedded Systems;
- Hardware technology (RFID, chips, sensors, routers, etc.);
- Human Machine Interface (HMI);
- Industrial Control Systems;
- Information Systems;
- Internet of Things;
- Mobile Devices;
- Operating Systems;
- Pervasive Systems;

- Robotics;
- Supply Chain.

#### 4.6.11 Challenge 2: Security hardening of supply chain infrastructures, including cyber and physical systems

Beyond the multiple physical assets that comprise the complex interconnected web of supply chain networks, there is another layer consisting of the complex interconnected web of IT and OT infrastructures and networks, which includes both legacy and cutting-edge systems, such as the cloud and the Internet of Things. All of these assets need to be continuously protected using a defence-in-depth strategy, which assumes the existence of successful attacks within the supply chain network that will actively try to hinder its operation, either directly or indirectly. As a result, as mentioned in the NIST framework for critical infrastructure cybersecurity [NIST 2018], it is necessary to provide protection to the whole asset lifecycle, from design to deployment, maintenance and recovery.

##### Specific Research Goals:

- ***Avoid complexities with the incorporation of security measures and services in IT-OT domains.*** The new trends to converge towards IT-OT domains and modernize the existing manufacturing infrastructures, bring the need to add new security solutions in terms of prevention, detection and response. But due to the heterogeneity of the context and the lack of standardization in this regard, the most recommended action would be to establish integration principles and standardized procedures following regulatory frameworks.
- ***Harden IT-OT infrastructures and perimeters according to the context.*** The incorporation of the new technologies and the convergence towards the IIoT/IoT, CPS and Edge bring the need to protect, from an adaptive standpoint, the current OT domains and to scale according to the infrastructural restrictions and the existing legacy HW/SW components and protocols. However, to achieve this interoperability and scalability level, it is also necessary to incorporate adaptive security measures (monitoring, intrusion detection, automatic response, recovery, etc.) that help promote an autonomous defence and resilience to network-level attack vectors.
- ***Harden software and hardware components following regulated procedures.*** Continuing with the two previous points, it is also essential to guarantee a HW and SW convergence in the industrial domains through a set of actions. One of these actions should be the provision of regulated and automated testing procedures to third parties' components; "security by design" for a secure boost, access control and data privacy (e.g. trusted computing platforms and trusted execution environment); and autonomous defence through machine-learning capacities.

##### JRC Cybersecurity Domain

- Software and Hardware Security Engineering;
  - Secure software architectures and design;
  - Runtime security verification and enforcement;
  - Continuous monitoring;
  - Security testing and validation;
  - Vulnerability discovery and penetration testing;

- Intrusion detection and honeypots;
- Malware analysis;
- Self-healing systems.
- Network and Distributed Systems
  - Network security (principles, methods, protocols, algorithms and technologies);
  - Distributed systems security;
  - Managerial, procedural and technical aspects of network security;
  - Network layer attacks and mitigation techniques;
  - Fault tolerant models;
  - Secure distributed computations;
  - Auditability and accountability;
  - Honey nets and honeypots.

### JRC Sectorial Dimensions:

- Energy;
- Health;
- Maritime;
- Transportation;
- Supply Chain;

### JRC Applications and Technologies Dimensions:

- Cloud and Virtualisation;
- Embedded Systems;
- Hardware technology (RFID, chips, sensors, routers, etc.);
- Human Machine Interface (HMI);
- Industrial Control Systems;
- Information Systems;
- Internet of Things;
- Mobile Devices;
- Operating Systems;
- Pervasive Systems;
- Robotics;
- Supply Chain.

#### 4.6.12 Challenge 3: Security and privacy of supply chain information assets and goods

One particular aspect of the supply chain ecosystem, whose importance demands the existence of a specific challenge, is the security and privacy of the information assets and goods. Within the supply chain ecosystem, all actors must access and exchange multiple types of information assets and goods, including private information about their internal processes for the implementation of various inventory management strategies (e.g. just-in-time) and information about the state of the transportation fleet, its cargo, and the

paperwork associated with this process. All of these assets and the management of their access control processes must be properly secured in order to avoid threats to confidentiality, integrity and availability, both physical and digital.

### Specific Research Goals:

- ***Specify a digital profile for all actors and products.*** As supply chain ecosystems are complex and intertwined, it is essential to develop a scalable federated identity ecosystem that will allow the identification and authentication of all stakeholders. This ecosystem can make use of advanced identity management solutions, such as self-sovereign identity.
- ***Provide a secure and privacy-aware data sharing infrastructure,*** which will allow multiple parties to share not only information about assets and goods, but also information about supply chain processes and events. All interactions should be stored for accountability purposes, and must only occur between authenticated partners, which will define their policies for accessing the information flow. As such, it should incorporate secure and privacy-enabled common interfaces and data types for the exchange of information. Moreover, the information infrastructure should be resilient against attacks in an environment with limited trust (e.g. using technologies such as blockchain).
- ***Facilitate the automatic analysis of shared elements such as information and process workflows.*** This will facilitate the discovery of exceptions and anomalies, including potential data leaks caused by inconsistent data sharing policies, the source of delays in complex workflows, and the potential presence of counterfeit products. It will also allow all entities to improve how they adapt and respond to issues in all supply chain processes (e.g. the transportation of assets and goods). This analysis can be based on simple mechanisms like rules, or in more complex solutions such as machine learning approaches.

### JRC Cybersecurity Domain:

- Data Security and Privacy
  - Privacy requirements for data management systems;
  - Design, implementation, and operation of data management systems that include security and privacy functions;
  - Pseudonymity;
  - Privacy by design and privacy-enhancing technologies (PET);
  - Data usage control.
- Identity and Access Management (IAM):
  - Identity management models, frameworks, services (e.g. identity federations, single-sign-on, public key infrastructure);
  - Authentication/Access control technologies (X509 certificates, RFIDs, biometrics, PKI smart cards, SRAM PUF, etc.);
  - Optical and electronic document security;
  - Legal aspects of identity management;
  - Law enforcement and identity management.

### JRC Sectorial Dimensions:

- Energy;

- Health;
- Maritime;
- Transportation;
- Supply Chain;

#### JRC Applications and Technologies Dimensions:

- Artificial intelligence;
- Big Data;
- Blockchain and Distributed Ledger Technology (DLT);
- Information Systems;
- Internet of Things;
- Pervasive Systems;
- Supply Chain.

#### 4.6.13 Challenge 4: Management of the certification of supply partners

Another aspect that is widely considered in existing recommendations and standards concerns the diverse procedures for the certification of potential and existing supply chain partners. This is related to security, because many items within these procedures are related to the security of the supply chain partner assets and processes. However, these certification processes pose various challenges. One is the complexity of the certification process, which involves auditing many assets and processes of all actors involved. Another challenge is related to the dynamic nature of a supply chain, where a certified partner might incorporate a weak link unknowingly after the process is finished.

#### Specific Research Goals:

- ***Automated mechanisms for the analysis of standard requirements and partner infrastructures.*** In order to facilitate the execution of the certification process, and due to its complexity, it is essential to develop mechanisms that not only extract the requirements of existing standards and recommendations, but also map such requirements to the existing elements of a particular partner – including its services, IT processes and assets – and provide additional recommendations to improve their compliance. This is a multidisciplinary challenge that involves information extraction from documents, analysis of IT/OT infrastructures, and recommender systems.
- ***Continuously monitor for compliance with standards and recommendations.*** For certain requirements of the certification process (e.g. IT/OT security), it is possible to make use of existing security and privacy tools to continuously analyse whether a certain partner is still compliant with such requirements. This research goal is related to some research goals specified in challenge 2 (Section 5.4.2), as the diverse tools that are used to audit the security of an infrastructure can also be used to continuously monitor the assets of such infrastructure. It is also related to challenge 3 (Section 5.4.3), as a secure and privacy-aware data sharing infrastructure is needed to share the results of these analyses.

#### JRC Cybersecurity Domain:

- Security Management and Governance;
  - Managerial aspects concerning information security;
  - Continuous monitoring;
  - Incident management and disaster recovery;
  - Reporting (e.g. disaster recovery and business continuity);
  - Assessment of information security effectiveness and degrees of control;
  - Adoption, use, and continuance of information security technologies and policies;
  - Vulnerability assessment and penetration testing (VAPT);
  - Compliance with information security and privacy policies, procedures, and regulations;
- Assurance, Audit, and Certification:
  - Assurance;
  - Audit;
  - Assessment;
  - Certification;
  - Protection Profile.

#### JRC Sectorial Dimensions:

- Energy;
- Health;
- Maritime;
- Transportation;
- Supply Chain;

#### JRC Applications and Technologies Dimensions:

- Artificial intelligence;
- Blockchain and Distributed Ledger Technology (DLT);
- Information Systems;
- Supply Chain.

## 4.7 Mapping of the Challenges to the Big Picture

This section provides a mapping between the security-related research challenges related to supply chains and the big picture of the supply chain ecosystem described in Section 5.1.

*Challenge 1: Detection and management of supply chain security risks.* As mentioned in the supply chain big picture, one of the main problems within the value chain is the integration and the convergence of “digital and ICT” elements into the operational tasks. Any vulnerability within their systems may certainly trigger an effect into the value processes that may impact on the business continuity. Therefore, this challenge aims to foster and establish adaptive security controls capable of dynamically detecting, tracking and evaluating risks.

*Challenge 2: Security hardening of supply chain infrastructures, including CPSs.* As discussed in the previous point, supply chain infrastructures converge towards the interconnection of hyper-connected IT-OT networks. This process inherently entails the need to harden the new connections, and create and make

sure trustworthy environments without impacting on the operational requirements such as real-time performance and business continuity at all times.

*Challenge 3: Security and privacy of supply chain information assets and goods.* As seen in the supply chain big picture, one of the core elements of supply chain ecosystems is information (about stakeholders, assets and goods, etc). Precisely, this challenge focuses on the protection of this information: from securing the integrity of the information itself to sharing and processing information in a secure and trusted way, so as to improve existing processes and enable new ones.

*Challenge 4: Management of the certification of supply partners.* Another main process reviewed in the supply chain big picture is the certification of stakeholders, which is used to provide proof of the quality and authenticity of their processes and products. This challenge is related to various aspects of this process, such as i) developing of automated mechanisms for the analysis of standard requirements and partner infrastructures, and ii) continuously monitoring IT-OT infrastructures to ensure that they are compliant with the certification requirements.

## 4.8 Methods, Mechanisms, and Tools

This section matches the relevant assets identified in WP3 with the challenges identified in the previous section, highlighting those methods, algorithms or tools that are necessary to lead the challenges.

### 4.8.1 Challenge 1: Risk management methodologies and frameworks

As stated by the NIST through its Cyber Supply Chain Risk Management (C-SCRM) program in [NIST 2019], the risk management methodologies for supply contexts based on complex IT-OT networks comprise a set of processes. These processes are mainly focused on identifying, assessing, and mitigating specific risks during the entire life cycle of a system (from its specification to its maintenance and destruction), mainly because any supply chain threat, anomaly and vulnerabilities may seriously impact on a subpart or the entire value chain.

Hence, the adaptation of standardized SCRM methodologies, guidelines and recommendations (e.g. NIST 800-161 [NIST 2015]), and the incorporation of risk assessment managers is critical to automatically:

- monitor and test the state of a context;
- extract conflict situations;
- classify risks according to threats and vulnerabilities (e.g. “adversarial”, such as tampering or counterfeits; “non-adversarial”, such as poor quality of parts, human errors or natural disasters; internal vulnerabilities associated with organizational/technical issues; and external vulnerabilities related to part of an organization’s supply chain); and
- evaluate them according to the states, dependencies and assets of the context.

With this, a system’s own risk management can help other protection systems make more accurate decisions and update the protection, security and defence engines against unforeseen situations and new threat vectors. Part of this automation also involves the incorporation of adaptive and dynamic threat modelling and risk assessment mechanisms specifically tailored to the needs of the supply chain sector.

The methodological tools for risk management proposed as part of WP3 and associated with its corresponding use cases in D5.1 are mainly related to “guidelines for GDPR-compliant user experience”. Therefore, more research is needed in order to provide automated and lightweight solutions based on particular SCRM for future IT-OT environments are still expected – note that this even goes beyond the application of existing general-purpose methodologies such as CORAS<sup>217</sup>.

#### 4.8.2 Challenge 2: Distributed detection, continuous monitoring and incident management

As part of defence-in-depth and the security criteria recommended by the JRC Cybersecurity Domain, detection in real time is one of the most extensive research areas in the literature today, since it allows one to know the state of a system and be aware of a situation. However, technological convergence towards OT networks (IT-OT) and Industry 4.0 implications in networks that are so constrained in operational and performance terms, means that the adaptation or the implementation of detection mechanisms is not so trivial as expected.

Detection mechanisms should be subject to lightweight approaches, be decoupled from operational tasks so as not to interfere with them, and be capable of interoperating with legacy devices from a distributed perspective. Apart from this, the operational conditions of the OT networks (e.g. response in real time, business continuity and ability to survive sophisticated attacks) require contemplating primordially “proactive” measures that allow the underlying system to detect and respond before major disruptions arise within the system. This also means that the prevention of 0-days exploitations and possible potential risks must, in turn, incorporate intelligent solutions capable of managing and warning of anomalies in real time, using, for example, intelligent algorithms such as data mining or machine-learning [ENISA 2019A]. These anomalies can be associated with network and endpoint risks, and may be derived from irregular operational behaviour or conducts (including human factor).

Therefore, the detection tools that can assist in this process corresponding to the second challenge “Security hardening of supply chain infrastructures, including cyber and physical systems” and according to the D3.1 are: Briareos and NextGen. However, more research is still necessary to guarantee optimal detection in supply chain contexts, taking into account the incorporation of:

- Lightweight distributed detection mechanisms composed of behavioural-based approaches and consensus-based algorithms, such as opinion dynamics or consensus algorithms.
- Proactive detection in order to ensure business continuity.

As part of prevention in real-time, it is also recommended to incorporate mechanisms that offer support in the incident management processes and in the tasks of correlation of events. Generally, these systems are supported by SIEM (Security Information and Event Management) systems as a protective measure. However, the level of coupling of security technologies should not entail the deployment of complex systems (e.g. with capacity for risk management, detection, response and cyber threat intelligence) that may cause serious computational, communication and storage penalties in operational tasks. So far there are

---

<sup>217</sup> <http://coras.sourceforge.net/>

insufficient assets identified in WP3 to cover the expectations for future industrial environments (containing diverse and specific industrial protocols). Only Briareos is the most representative tool in this sense.

### 4.8.3 Challenge 3: Traceability, Shared Data Spaces

#### Traceability, auditing and accountability of assets and goods

The traceability of assets and goods is one of the core services of the supply chain ecosystem. At present, there are multiple software platforms and hardware tools, such as RFID tags and GPS tracking units, that integrate these assets into IT infrastructures, allowing all actors to monitor in real-time their location and status. Some companies are also adopting blockchain-based solutions to solve basic supply chain problems like tracing each product (e.g. pork meat, precious stones) to its source. Nevertheless, it is necessary to provide additional solutions that take into consideration the current landscape of complex multi-tiered supply chains with multiple parties. These solutions should provide the following services:

- Deployment of a digital profile for all actors and products, using technologies such as certificates and the Internet of Things.
- Blockchain-based smart contracts to monitor and manage exceptions proactively (e.g. invalid parameter thresholds, inconsistencies between sales order and purchase order).
- Automatic registration and sharing of supply chain events between interested parties.
- Exchange of private data with accountability through cryptographic hashes.
- Streamlining of compliance requirements and clearance processes.
- Integration of automatic analysis mechanisms for the detection of tampered goods.

Note that certain tools developed in WP3 can be used to meet the research challenges associated with this area. The deployment of self-sovereign identity management approaches based on the blockchain can facilitate the integration and interaction of new partners in a complex supply chain ecosystem. Other assets like Cryptovault can be used for the privacy- and integrity-preserving storage of critical information. Finally, all mechanisms can benefit from an analysis of interoperability and cross-border compliance issues for the interoperability of identity technologies.

#### Supply chain shared data space

In today's supply chains, existing ERP components already enable the creation of data spaces that are shared between suppliers and providers, facilitating the implementation of various lean production techniques. However, it has previously been determined that concerns regarding data confidentiality and unauthorized usage represent one of the major barriers preventing stakeholders from integrating their information in common shared data spaces. This is more critical in ecosystems like Industry 4.0, where various partners will interact in a dynamic context. It is then necessary to create a safe and secure shared data space that achieves a balance between information security (secure, controllable and trusted environment) and information accessibility (usable interfaces and generic data exchange formats). The mechanisms that could facilitate the creation of such shared data spaces in complex environments must then provide the following functionality:

- Secure infrastructure that facilitates the interaction between authenticated stakeholders in a federated ecosystem.
- Definition of easily configurable access control and data sharing policies.
- Trust mechanisms that facilitate the interactions between stakeholders.
- Automatic mechanisms that analyse the infrastructure in order to uncover potential anomalies (e.g. inconsistent data sharing policies, unwanted data leaks).

One of the tools introduced in WP3 that can improve privacy in the exchange of this information is privacy-preserving middleware components, which can be deployed at a local level, at the edge, or in the cloud. These components can integrate various privacy policies, which define various aspects such as how and when the information can be shared, and what privacy-enhancing technologies should be applied. Other tools, such as PLEAK<sup>218</sup>, can help in selecting specific privacy parameters and policies.

#### 4.8.4 Challenge 4: Continuous Certification

Both suppliers and providers make use of certification programs (e.g. O-TTPS certification program) to assure customers of the integrity of their supply chain infrastructure. Many aspects of these certification programs focus on assessing the security of IT infrastructures, services and goods. One potential approach to enrich this certification process is not to rely on the certification of a supply partner and its components at a particular point of time, but to rely on the execution of several continuous processes that take into consideration the dynamic nature of this particular scenario. This way, all partners are encouraged to continuously improve their security processes. Some of the mechanisms that could facilitate this ongoing process have already been defined in the “Distributed detection, continuous monitoring and incident management” section related to the second challenge. Other mechanisms that can help to implement this idea are as follows:

- Automated penetration testing frameworks analysing live copies of the supply chain IT infrastructure (e.g. digital twins).
- Firmware, software, and configuration analysis tools (e.g. fuzzing) for the analysis of hardware and software assets.
- Tools for sharing threat intelligence between partners.

As in the second challenge, certain WP3 tools like Briareos can be used as a foundation for the deployment of continuous certification platforms.

Table 3: Challenges identified in the Supply Chain Vertical and Tools needed to address them

Challenge	Tools required for	Tools contemplated for Supply Chain	Tools/Methods that need to be addressed
Challenge 1	Risk management methodologies	Guidelines for GDPR compliant user experience (D3.1, Section 5), and general-purpose	Adaptation of recognized SCRM methodologies, lightweight and automated mechanisms for supply chain scenarios

<sup>218</sup> <https://pleak.io/home>

		methodologies such as CORAS (D3.1, Section 5.2)	
Challenge 2	Detection, Continuous monitoring and incident management	Briareos (D3.1, Section 5.3) and NextGen (D3.1, Section 5.3)	Behavioural-based approaches and consensus-based algorithms, and proactive detection through machine-learning or data-mining. Lightweight SIEMs with ability to contemplate the specific complexities of the context
Challenge 3	Traceability	Self-sovereign identity management (D3.1, Section 5.1), Cryptovault (D3.1, Section 5.1)	Digital profile for actors/assets, blockchain-based smart contracts and events, automatic analysis mechanisms
Challenge 3	Shared data spaces	Privacy-preserving middleware (D3.1, Section 5.6), PLEAK (D3.1, Section 5.6)	Secure shared data space infrastructure with access control and data policies
Challenge 4	Continuous certification	Briareos (D3.1, Section 5.3)	Penetration testing, security analysis tools, threat intelligence

## 4.9 Roadmap

### 4.9.1 Short-term plan

According to the latest ENISA report on the “*threat landscape for supply chains*”,<sup>219</sup> the number of global threats to the supply chain has been increasing during the last two years (2020 and 2021) with a relevant APT presence (APT29 and AP41). Most of the attacks correspond to unknown threats, exploits to software vulnerabilities of the supply chain (such as code, data and processes), or malware injection. Thus, for the remaining months until the end of the project we need to focus on the “*software supply chain*” protection, comprising the following aspects related to supply chain security:

- 1 It is still necessary to continue working on and researching applications that facilitate **supply chain risk management**, especially addressing those related to supply chain “cybersecurity” risks. This process includes, among others: the specification and analysis of cyber kill chains that will highlight the weakest points in the supply chain ecosystem and manage fraud, and the definition and establishment of continuous vulnerability analysis processes that, based on different stakeholders, services and (inter-)dependencies, monitor the compliance of certain supply chain processes.
- 2 **Exchange of trusted information among stakeholders**. More progress still needs to be made in the area of information sharing, raising awareness of cybersecurity and privacy issues and establishing obligations and responsibilities in this regard. Both aspects provide a foundation for the security of the software supply chain, where the creation of trustworthy interactions between stakeholders is critical

<sup>219</sup> ENISA, “Threat Landscape for Supply Chain Attacks”, <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>, July 2021.

to safeguard future risks. At this point, ***governance under well-defined regulatory frameworks and monitoring of security*** are also two key aspects that should be relevant in this short-term period.

- 3 In relation to governance, ***security audits*** are also essential ***to verify compliance with cyber security principles and responsibilities throughout the supply chain***. All information generated from supplier influences and interactions, use of and access to private data, and good practises should be accessible, so that this information can be easily readable and traceable. One of the most prominent technologies that can currently address this need in the coming months is the ***Distributed Ledger Technology*** (DTL). Within DTL, blockchain-based solutions could be a good approach to show their usefulness until the end of the project; mainly because there are various avenues that can be explored in this period of time, and especially in the research actions carried out in WP5 (see in Section 4.9.3 the two use cases defined: SCH-UC1 and SCH-UC2). For example, one such avenue is the ***integration and verification of accountability protocols*** that could be used in case of conflict, where trusted third parties can manually review the workflow and resolve conflicts if it is apparent that an entity has not behaved according to the established rules. Another avenue is related to ***exploring the integration of GDPR enforcement solutions***, where processes and workflows implemented in the blockchain can comply with existing regulations. Other aspects include ***self-sovereign identity solutions***, and ***the exchange of private data through various means***.

## 4.9.2 Beyond the end of the project plan

### 4.9.2.1 Security 2025

In the supply chain domain (and in terms of goods, hardware and software), there will be some research priorities that will need to be covered by 2025. They are as follows:

1. In the previous section, risk management was described as a primary input to be considered in the short term. However, this management in the next four years should be sufficiently automated and dynamic to provide better support throughout the supply chain, and better feedback for the rest of the mechanisms that are part of security, such as intrusion detection or prevention systems, SIEMs and SOCs. The integration of these automatic analysis mechanisms can also be useful for other security purposes, including: (i) the ***integration of continuous certification processes*** that can attest to the security of supply chain infrastructure, hardware assets and goods, and software assets and goods; and (ii) the ***implementation of better supply chain risk management policies*** that consider not only a failure in Tier 1 partners but also potential cascade effect issues; in addition to (iii) ***intensifying the situational awareness in the entire value chain***. Therefore, more research is expected to be done on ***“dynamic and automated” risk management*** with the ability to continuously analyse and pinpoint potential and/or existing security and privacy issues in all assets, while subject to regulations as aforementioned.
2. In connection with dynamic risk management, it is also essential to ***automate the (zero-days) vulnerability management*** according to security controls. These controls involve aspects like the persistent monitoring of trustworthy sources under requirements of exchange of trusted information, and the identification, application and verification of security patches.
3. Although there are already research attempts to provide protection to the IT/OT infrastructure of supply chains through defence mechanisms (e.g. prevention through cloud, PUF and blockchain technologies), there is still a need to provide automated and advanced security measures that ensure the ***secure production and distribution of supply chain goods***, including both software and

hardware assets, ***under regulated and controlled (cyber)security practises***. This implies that all the technological dependencies should be based on: (i) *robust and resilient systems and infrastructures*, (ii) *secure and integral software components*, and (iii) *suitable protection tools and mechanisms that can provide advanced security measures*. These measures can range from penetration testing to automated software analysis services, including firmware, security patches, middleware, software development platforms, virtualization systems and open source components. The introduction of certifications and guidelines in this regard will also push the integration of such mechanisms into existing supply chains.

4. ***Future security approaches can take full advantage of emerging technologies to improve their processes***. For example, leveraging the decentralised properties and capabilities of DLT-based technologies to fulfil their purpose as a mechanism that can be applied to protect the security and privacy of all assets and property. The mechanisms that are needed to fulfil this goal include the *exchange of data between different blockchains*, the *execution of automated tasks* (outside or inside various blockchains) *to automatically monitor the state of a complex interconnected supply chain*, *a deeper integration with existing frameworks* (such as compliance requirements and clearance processes), and *the implementation of self-sovereign identity approaches to manage certain actors and assets of supply chains*. Likewise, 5G-based supply chain infrastructures can enable the *transmission of low-latency mobile data information, favouring the management of preventive processes* that security mechanisms normally require to function properly (e.g. to improve real-time connections for online cyberdefense).

#### 4.9.2.2 Security 2030

In the supply chain domain (and in terms of goods, hardware and software), there will be some research priorities that will need to be covered by 2030. They are as follows:

1. ***Further and broader coordination and regulation of Europe's own supply chains of hardware and software assets*** in order not only to establish competitive positions with respect to other countries, but also to create a reliable and trustworthy adaptation of future technological deployments corresponding to Industry 5.0 (and next generations), such as 5G/6G (B6G), drones and autonomous vehicles, digital twins, quantum computing, AI and Big Data. This will also require further research, development and implementation of security methods, defence strategies, infrastructures, platforms and/or legislation that are also expected to ***promote supply chains under secure-by-design principles***.
2. Concerning the previous point, the ***advent of AI and Big Data in Industry 5.0 (and next generations) and applied to IT-OT infrastructure security and privacy***, in addition to other tools such as ***threat intelligence sharing***, undoubtedly provides multiple benefits to supply chain infrastructures, including: (i) *optimising and improving decision-making and response processes for cyber intelligence, to achieve better situational awareness and better system governance*; and (ii) *automatically hardening supply chain IT-OT infrastructures through improved knowledge of the infrastructure and its risks*. But the introduction of these technologies must not hinder the continuity of the value chain or jeopardise the privacy of its stakeholders.
3. ***Optimised traceability (and connected transparency)*** is an important issue in supply chains for tracking the products/resources themselves (including software), but ***“adapted” and based on the***

*development of modern life and its implicit problems.* For example, it will also be important for emissions tracking purposes, as evidence of the use of sustainable and responsible materials and practises, prevention of counterfeiting and prevention of exploitation of labour. While at least some of these are likely to become legal requirements, this will also have the advantage of providing the consumer with better information on the origin of a product, which may provide a commercial advantage over competitors. For all of this to be possible, sophisticated and reliable traceability/transparency solutions are paramount.

At this point, research about the role of blockchain technology together with AI could be key in order to find and *provide adaptive traceability and transparency solutions.*

4. The EU should initiate coordinated actions and introduce supply chain security standards and regulations to compel organisations to comply with supply chain security measures and to protect the EU’s sovereignty, including digital sovereignty. For example, the regulation could define and require organisations of a certain size or those in specific/crucial industries to ensure supply chain integrity. Hence, the EU should *launch new and/or support existing initiatives that focus on securing supply chains in certain sectors or across sectors.*
5. *Availability of autonomous self-healing processes*, which will facilitate the automatic recovery and reconfiguration of states, processes or parameters in cyber-physical systems and IT-OT networks in optimal times—an essential aspect to guarantee at all times business continuity in (hyper-)connected supply chain networks.

Within the response and recovery/reconfiguration fields, some research priorities should be solved by 2030 such as: (i) *how to achieve automatic recovery/reconfiguration of supply chain systems or infrastructures in linear times (or almost in linear times); and (ii) how to coordinate automatic response within a sector or across sectors.* One technology that can manage and facilitate these issues are the *“smart” (and distributed) digital twins*, which could make possible both the prediction and reconfiguration of the system. Still, there are various research challenges associated with this concept, including: (i) *how to manage “trust” in the two-way interface; and (ii) how to trust automatic responses in critical supply chain domains.*

### 4.9.3 Milestones

By the end of the project, CyberSec4Europe will reach the following milestones regarding the development of reusable assets and demonstrators for real-life use cases.

- Blockchain platform and consensus algorithm
- Workflow compliance assurance and accountability
- Dispute Resolution for Retail Supply Chain
- Compliance and Accountability in Distributed Manufacturing:

## 4.10 Summary

This section focused on the security of the supply chain. As explained the supply chain sector is under attack by criminal organizations, intelligent services, insiders, and even terrorists. In fact, we have shown in section 4.5 that these major incidents in this vertical have mainly focused on the acquisition of data, theft, and sabotage. As explained in section 4.3.3, and as described in 4.5, such incidents can deliver a major blow which can result in harm to operations, harm to assets, harm to individuals, and potentially even harm to entire nations!

After a review of the state of the art in this area (cf. section 4.6.1), a brief SWOT Analysis in section 4.6.2 showed that EU has the capacity to lead research in this area and has already made investments towards this direction. On the other hand, lack of leadership, international resistance, and lack of relevant security standards, may jeopardize any ongoing and future efforts. We see a clear opportunity for Europe to take a leadership in promoting (i) a global approach and (ii) a supply chain security standardisation effort.

Additionally, we have reviewed how there are various aspects, or dimensions, that we have to consider when protecting global supply chains - either physical or digital. Some of these dimensions, such as the COVID-19 and public health dimensions (section 4.6.4) have shown various weaknesses in this vertical, such as the increased attack surface due to the dynamic nature of supply chains, that must be carefully considered. Other dimensions, like the green and climate change dimensions (sections 4.6.5, 4.6.6), have shown how the digitalisation of supply chains can contribute to the EU roadmaps that focus on protecting the environment and ecosystems worldwide through optimization and environmental impact tracing.

Finally, the recent pandemic reminded us that the security (integrity, confidentiality, and availability) of the supply chain is of paramount importance for the European Digital Sovereignty (see sections 4.6.3, 4.6.7): fake news, fake medicines, unavailable services, and buggy software are only the tip of the iceberg that cripple the security of the supply chain and undermine European Digital Sovereignty. Moreover, we have described how the security of supply chains aligns with the EU CyberSecurity Strategy for the Digital Decade in various aspects (cf. section 4.6.10).

We have to admit that the situation was bad and became even worse. To try to address the issue we have identified four major research challenges (cf. sections 4.6.11 – 4.6.14):

- Challenge 1: Detection and management of supply chain security risks
- Challenge 2: Security hardening of supply chain infrastructures, including cyber and physical systems
- Challenge 3: Security and privacy of supply chain information assets and goods
- Challenge 4: Management of the certification of supply partners
- In order to address them, there are various aspects that must be given priority for the next years (cf. section 4.9). **In the short term**, we need to continue working and researching on applications that facilitate *supply chain risk management, exchange of trusted information among stakeholders, governance under well-defined regulatory frameworks and monitoring of security, and verification of compliance with cyber security principles and responsibilities throughout the supply chain*. Regarding the research priorities that need to be **covered by 2025**, more research is expected to be done on *“dynamic and automated” risk management, automated management of (zero-days) vulnerabilities, advanced security measures for the secure production and distribution of supply chain goods under regulated and controlled (cyber)security practises, and usage of emerging technologies such as DLT-based technologies and 5G (and beyond)*. Finally, if we think on long term research that needs to be **covered by 2030**, we should think of *further and broader coordination and regulation of Europe's own supply chains of hardware and software assets, the application of AI and Big Data in Industry 5.0 (and next generations), optimised traceability (and connected transparency), launching new and/or support existing initiatives that focus on securing*

*supply chains in certain sectors or across sectors, and the availability of autonomous self-healing processes.*

## 5 Privacy-Preserving Identity Management

### 5.1 The Big Picture

The identity management scenario involves various actors with different goals. **Users** want to make use of services or protected resources. They are characterized by different attributes that make up their identity, which may be grouped in subsets to form partial identities. For privacy-preserving identity management, it is precisely that identity data and the user activity that must be protected. **Service providers** (or **relying parties**) offer various services and are in charge of the safeguard of the resources. They need to verify that users meet the necessary conditions to grant them the access they request. The requirement can be simply knowing the account credentials (e.g. the widespread username and password), or include some constraints over the user attributes. For this verification process, **issuers** (or **identity providers**) are commonly used as a source of trust. The service provider can verify the validity of the user's claims over his/her identity because a trusted issuer attests them.

Thus, the key process in identity management is the authentication/authorization, where users gain access to some service or resource by proving to the service provider that they meet the required conditions. It may be preceded by an issuance process, where one or multiple issuers give the users the attestations necessary to prove their identity. In these processes, different components are involved, like the issued attestations (e.g. credentials, certificates), the user's tools to manage them (e.g. wallets), and the claims that have to be verified by the service provider (the certificates themselves or proofs over them). Also, with new trends for identity management, more components may be introduced, including distributed ledgers that give support for decentralized identifiers, resolution of public identities and information or other specific services like credential revocation.

In this scope, privacy-preserving Identity Management (ppIdM) refers to the provision of secure and trustworthy online identity management capabilities to users and entities so they can safely interact (i.e., mechanisms for authentication/authorization must be provided as they are needed for those interactions) while exercising their rights regarding privacy. In this sense, regulations like GDPR are very relevant, establishing principles like data minimization, right to be forgotten or strict laws about user consent.

### 5.2 Overview

Current authentication and identity management (IdM) mechanisms have difficulty meeting the necessary security and privacy requirements while maintaining acceptable usability levels. Single sign-on (SSO) systems [De Clercq 2002], based on technologies such as OAuth (Open Authorization) [Hardt 2012] or SAML (Security Assertion Markup Language) [CMJ 2015], have barely evolved and suffer from several drawbacks for managing identity information in a reliable and privacy-preserving manner. At best, websites verify email addresses and phone numbers by sending one-time codes: e.g. a user registering on a social network like Facebook will receive a one-time verification SMS to validate his/her mobile phone and email. Age verification, which should be a common use case given the amount of age-restricted material offered online, is usually performed by verifying a credit card number, even though credit cards were never meant for this purpose and are also available to teenagers in many countries.

Several countries have started issuing electronic identity cards in an attempt to remedy this situation. Electronic identity cards usually come in the form of smart cards that are cumbersome to use in combination with personal electronic devices, such as phones, tablets, and laptops. Moreover, national identity cards from different countries are usually incompatible, forcing web services to choose which countries they want to support [TSR 2003].

Among the plethora of technologies and possible solutions, traditional credentials based on usernames and passwords are still the most popular way to authenticate users online and, besides the annoyance of having to supply the same information several times to different parties, the main issue with this is how the information is protected at these sites. Data breaches have reached a new high in the last few years, and billions of user records have been exposed, leading to numerous cases of identity theft and impersonation; this makes the need to move on from the password paradigm more imperative than ever.

The trivial approach to account management is to pick a username and password for each account and then upload their relevant attributes to the provider. However, this entails significant issues in relation to breaches and linkability. Not all providers have the same level of concern for the user's personal information. Despite the risk of heavy fines through legislation such as the General Data Protection Regulation (GDPR) [PvdB 2017], some providers may not implement effective protocols in order to ensure the security of personal data. This in turn might lead, either due to negligence or due to financial motivation, in leakage of users' personal information. Since the traditional username and password approach can no longer satisfy the needs of contemporary users in terms of both security and usability, it is clear that new standards need to be adopted that leverage all the benefits that the latest industry trends have to offer. Other technologies are appearing, such as distributed ledger technologies (DLTs); specifically, blockchain is undergoing rapid adoption and its popularity is growing thanks to promises of scalability, security, immutability, etc. However, this type of technology also suffers from privacy issues, with the aggravating circumstance that records are assumed to be perennial [BBC 2019].

With all of this, and despite privacy regulations and user awareness, there is a lack of reliable and privacy-preserving self-sovereign IdMs and solutions applicable to distributed DLTs that would empower users with full control over their identities in diverse scenarios while addressing identity related threats.

There is a need for IdM systems that address identity management in a holistic way, encompassing identity proofing, identity derivation, strong password-less and multi-factor authentication, privacy-preserving attribute proving, as well as supporting cyber-crime prevention and incident investigation. In addition, existing mobile identity solutions lack assurance mechanisms based on identity derivation from official physical breeder documents (ePassport and national eIDs<sup>220</sup>) that would provide sufficient trust.

Regulation (EU) 2016/679<sup>221</sup> of the European Parliament and of the Council, more commonly known as the GDPR, is a legal framework that sets guidelines for the collection and processing of personal data. This is arguably the most significant change in data privacy regulation in the last few decades. The regulation applies across the entire European Union (EU) and European Economic Area (EEA). While the regulation does not mention identity management or the related access management directly, according to one survey

---

<sup>220</sup> Electronic IDentities

<sup>221</sup> <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

[Hobson 2020] half of the companies agree that GDPR compliance is not possible without it. Naturally, IdM systems in use must themselves follow the GDPR requirements for compliance to be possible.

Regulation (EU) No 910/2014<sup>222</sup> of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, more commonly known as eIDAS, is a fairly recent (23 July, 2014) regulation on electronic identification and trust services in the European Single Market. The trust services mentioned include electronic signatures, electronic seals, time stamps, electronic delivery services and authentication. Together with electronic identification, they allow for trust, security and legal certainty in electronic transactions. This regulation applies across the entire European Union (EU) and European Economic Area (EEA). Ultimately the eIDAS regulation will ensure that all Member States offering an online public service for which access is based on an electronic identification scheme will also recognise the electronic identification of other Member States.

## 5.3 What is at stake?

### 5.3.1 What needs to be protected?

**Services and implementations.** A (privacy-preserving) identity management system involves a variety of parties, including issuers, relying parties, potential authentication service providers, as well as users. The security of the entire system rests on the security of its weakest link, as a compromise of either participant can cause a negative impact on all other entities in the ecosystem. Thus, secure protocol designs, implementations and deployments are needed.

**Access to key material.** Related to the above, access to any type of secret key material of any party (encryption keys, credentials, signing keys, etc.) can subvert the security of the entire system. Access to all secret key material thus needs to be protected by physical (e.g. hardened devices) but also logical (e.g. security architecture) means.

### 5.3.2 What is expected to go wrong?

Below, we summarize the main threats and security risks in the context of privacy-preserving authentication. For further reading, we refer, e.g. to ENISA<sup>223</sup>.

**Identity theft.** Users' private data, such as encryption keys, personal credentials or even biometric data, can be exposed to an adversary as a result of flawed protocol designs, insecure implementations, hardware faults, inappropriate protection on the user's side (e.g. through weak passwords), etc. As a result of successful identity theft, an attacker could fully take over a user's digital identity in different contexts, underlining the severity of this attack.

---

<sup>222</sup> [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L\\_.2014.257.01.0073.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG)

<sup>223</sup> ENISA: "Mobile Identity Management", 2010. Available at <https://www.enisa.europa.eu/publications/Mobile%20IDM>

**Phishing.** This is the process of gaining a user's trust (and thus access to sensitive authentication information) through mimicking a trusted entity. Such attacks can be performed on different levels (network, software, email, etc.). Typical attack scenarios are related to bank accounts.

**Forgery.** Insecure implementation or faulty protocol design may enable users to undermine the authenticity of the authentication process. In this case, malicious users can successfully authenticate without having access to valid authentication data such as cryptographic key material, biometrics, etc. As a result, an attacker may either consume a service illegitimately or gain access to another user's account.

**Subverting business models.** Depending on the protocol design, its implementation, and whether or not authentication is bound to a hardware token (e.g. a trusted platform module), it may be possible for users to share their accounts. In particular, this is a risk if users do not need to share their entire, e.g. credential or key material, but can perform single authentication sessions on behalf of another user. For instance, if user A wants to authenticate in a challenge-response based scheme, he/she might forward the challenge to user B (holding a valid authentication token), receive the response from B, and forward it back to the relying party. In this case, B does not need to share any sensitive information with A, while A does not need to buy a potentially expensive subscription for the service. It is worth noting that this kind of attack is typically not considered in the cryptographic analysis of authentication schemes.

**Data leak.** Service providers may store significant amounts of sensitive user data, such as attributes or metadata, to improve their offers and business models, or because of legal requirements. Depending on how this data is stored and protected, it may leak through improper hardware disposal, misconfigurations of the system, or because of attacks by internal or external actors.

**User identity and attributes.** In case of bad protocol design, implementation flaws, etc., the unique identity of a user, or specific attributes of a user (e.g. name, date of birth, etc.) participating in an authentication session might become exposed to any of the other parties participating in the protocol.

**Linkability and profiling.** In case of a bad protocol design, implementation flaws, etc., different actions taken by the same user may be leaked to any of the other entities participating in the protocol, or even to an outside adversary (cf. also ISO/IEC 27551 for different unlinkability levels), without the user's consent. This metadata might allow for detailed profiling of a user, potentially also revealing his/her unique identity.

**Extortion.** If a relying party or identity provider gains knowledge of sensitive user information, this information may render the user vulnerable to extortion. The same may apply in the case of a data leak, e.g. due to a hack by an intruder.

**Surveillance.** Analysing network traffic, source and destination addresses, etc., may pose the risk of monitoring and surveillance, even if the transmitted content is properly protected. Such an attack can lead to the unintended disclosure of large amounts of personal information and provide a detailed profile of an unsuspecting user. Mitigating this problem requires protection not only at the application level, but also at the network level.

**Denial of service.** Many authentication scenarios mandate the possibility of revoking authentication credentials, e.g. by the issuer or the relying party. On the downside, this might also give the party administering the revocation lists (e.g. blacklists of revoked credentials), the option to invalidate a user's credential maliciously.

**Real-world implications.** While the previous risks focused mainly on digital attacks, we want to stress that these can also lead to relevant implications in the physical world. For instance, if authentication sessions can be linked to a smart home device, it may become possible to infer whether a user is currently at home or not. Or if sessions of a medical device can be linked, it may become possible to infer that a user has certain medical conditions.

### 5.3.3 What is the worst thing that can happen?

In the case that no further research is done, and existing research results are not successfully pushed into large-scale deployments, it is to be expected that non-privacy-preserving identity management solutions will stay in place and will be further deployed by major companies and governments.

Besides the aforementioned risks, this might lead to large-scale mass surveillance, by private companies, criminal organizations or public authorities, with all the potential negative implications if the collected data is used against the users or citizens (e.g. if the data is used as a basis for social credit systems). We want to stress here that this mass surveillance and analysis of the data can easily be scaled to entire nations and beyond, posing a severe risk with real world implications for potentially billions of users of large-scale cloud services.

## 5.4 Who are the attackers?

We next define specific types of attackers for privacy-preserving identity management systems. Here we only focus on generic attackers, but do not consider attackers that are specific to the context in which the authentication scheme is being used.

On a high level, we distinguish two types of attackers: internal and external. Internal attackers are all parties participating in the ecosystem of the authentication scheme under consideration (e.g. issuers, relying parties, etc.), while external attackers are not part of this ecosystem.

**Users (internal).** Users can have different incentives to attack the system. Firstly, they can aim to pass identity verifications without having the corresponding attributes, e.g. they try to access an age-restricted service without being the correct age. Secondly, they can try to authenticate towards a service without having any corresponding credentials at all. Finally, users can try to sell/forward authentication requests to other users, e.g. for monetary reasons.

**Relying party (internal).** Relying parties or service providers may aim to break the privacy guarantees of the authentication mechanism in order to trace the user. In addition, they may request more information than required for authenticating a user, and they might extensively store and process information beyond the stated purpose. Relying parties may collude with other entities (e.g. issuers, authentication service providers) to achieve this goal.

**Issuer (internal).** Issuers may wish to trace users for various reasons, e.g. because of their business model. This is specifically relevant when the issuer is involved in the authentication protocol itself (e.g. “calling home”). The issuer may collude with other entities (relying parties, authentication service providers) to achieve this goal.

We stress that this collaboration with other roles in the ecosystem occurs naturally in many cases, where issuer and relying party are actually the same entity, e.g. in the case where an online service issues subscription certificates, and users later on authenticate towards the same service provider to consume the service.

**Authentication service provider** (internal). This entity only exists if the authentication process is (partially) outsourced to the cloud, and not all computations (e.g. cryptographic operations) are locally performed by the user. Similarly to the above, authentication service providers may wish to trace users, e.g. for business reasons, store information beyond the claimed purpose, or perform other suspect operations. Authentication service providers may collude with other entities (relying parties, issuers) to achieve this goal.

**Disgruntled employee** (internal). Current or former employees (of issuers, authentication service providers, relying parties, etc.) who wish to damage the company or its reputation may maliciously leak data containing sensitive user information to the public.

**Competing users** (internal/external). In order to compromise a competing user (e.g. in political debates), users may aim to obtain sensitive information about a user from other entities in the ecosystem.

**Ruthless competitor** (internal/external). Competitors may wish to steal information from their peers (e.g. relying parties) for various reasons. On the one hand, the obtained information could be used to improve their own products. On the other hand, and with a higher impact for the affected users, they may leak the information to the public to harm their competitors.

**Public authorities** (external). While typically not being considered “attackers”, public authorities or law enforcement agencies may have incentives for different types of attacks on authentication processes. For instance, they may enforce the placement of trapdoors in cryptographic mechanisms in order to allow for tracing individual users or large groups of users for surveillance purposes, thereby posing a risk not only to the specific users but to the ecosystem as a whole.

**Hackers** (external). Cyber-criminals may aim at hacking any party in the system for their own advantage. Information obtained from issuers, relying parties, or authentication service providers may be abused to blackmail these entities or the users whose information was disclosed. Attacking users, e.g. through spear phishing, can lead to identity theft and corresponding harm for the user.

## 5.5 Major incidents in this vertical

The large amounts of data being managed in digital interactions have only been increasing in recent years, and this trend seems unlikely to stop (rather the opposite). This has led to many grave incidents where sensitive data has been stolen, leading to privacy breaches at best, and breaches which provoked further criminal acts (e.g. theft) at worst. Some relevant instances have been:

- **ChoicePoint 2005.** Personal financial records of more than 163,000 consumers were compromised and at least 800 were used for identity theft. This sensitive data was extracted by the thieves through

false requests that were not adequately checked for legitimate purpose and validity. Moreover, these mass requests had been detected and reported but no action was taken against them.<sup>224</sup>

- **Sony PlayStation 2011.** Personal information, including names, birthdates, passwords and potentially credit card information of PlayStation Network users stored by Sony. Allegedly (reported by Sony with some proof but not definitive) the theft was carried out by the group *Anonymous* using Denial of Service (DoS) as a screen for other cyberattacks that have not been disclosed.<sup>225</sup>
- **Google exposed user data 2015-2018.** The giant exposed (through its social network Google+, which had a glitch which let developers access sensitive data from users without proper authorization) the private data of hundreds of thousands of users and hid the information about the breach [MM 2018].
- **Many other leaks of accounts, passwords and personal information stored by service providers,** affecting, to name a few, Adobe<sup>226</sup> and Dropbox. The latter is an interesting case, as it was (allegedly) a result of another breach from LinkedIn and one of Dropbox's employees reusing its password, exemplifying the threat this kind of reuse poses.<sup>227</sup>
- Apart from this kind of incident, one of the best-known events regarding privacy was the **leaks of global surveillance by Edward Snowden from 2013.**<sup>228</sup> This highlighted the massive amounts of data and privacy breaches committed by governmental bodies, in this case specific to the NSA in the USA, though other countries have also been known to perform massive surveillance operations.
- Lastly, we find it important to remark that the potentially gravest privacy breaches are not one-time events but the result of the continuous collection of personal data. Indeed, current business models are often centred around obtaining and processing massive amounts of user data. This is the case for the biggest companies, which are a staple of people's everyday lives and have been involved in many scandals relating to privacy. For instance, **Google** and **Facebook** are frequently involved in this kind of incident, be it in a "lawful" but invasive manner (as exemplified by the article regarding the former we refer here<sup>229</sup>) or through unconsented and unlawful practices (as it appears in the selected article about the latter<sup>230</sup>). This is especially relevant for this vertical, as the identity

<sup>224</sup><https://www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million>

<sup>225</sup> <https://www.telegraph.co.uk/technology/sony/8494177/PlayStation-hack-Sony-blames-Anonymous-hacktivists.html> and <https://www.telegraph.co.uk/technology/sony/8495072/Playstation-hack-timeline-of-huge-security-breach.html>

<sup>226</sup> <https://www.nytimes.com/2013/10/04/technology/adobe-announces-security-breach.html>

<sup>227</sup> <https://www.techrepublic.com/article/2012-dropbox-hack-worse-than-realized-68m-passwords-leaked/>

<https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach>

<sup>228</sup> <https://www.businessinsider.com/snowden-leaks-timeline-2016-9>

<sup>229</sup> <https://www.cnet.com/tech/services-and-software/google-collects-a-frightening-amount-of-data-about-you-you-can-find-and-delete-it-now/>

<sup>230</sup> <https://www.independent.co.uk/news/world/americas/facebook-data-privacy-scandal-settlement-cambridge-analytica-court-a9003106.html>

management solutions controlled by these two companies (Single-Sign On) are currently the most used.

## 5.6 Research Challenges

### 5.6.1 State of the Art

The previous version of the “Research and Development Roadmap” [Markatos 2020] initially identified the main elements in the field of the ppIdM with regard to cybersecurity, the security requirements of the domain’s critical infrastructure, who the attackers are and their profile. In addition, a set of security challenges and issues were raised in the area of ppIdM; these issues and challenges are defined in the following sections 5.5.6 – 5.5.10. This section represents the range of research that best captures the state of the art in ppIdM with respect to the challenges posed. A description of the state of the art in ppIdM before the project started one year ago can be found in other deliverables, such as D3.11 [Sforzin 2020].

#### 5.6.1.1 System-based credential hardening

The first known attempt at hardening passwords using a cryptographic service was deployed by Facebook [Muffet 2019] and was based on applying several rounds of hashing and MACs in a single password. This prompted a series of research proposals based on more elaborate services for password hardening. We discuss here the most popular proposed schemes.

Pythia [ECS+ 2015] is based on using pseudorandom functions (PRF), for instance an HMAC, instead of typical hashing. For cracking passwords, if Pythia is in place, you need access to the key involved in the PRF; for instance, the internal key used in the HMAC computation. Pythia cannot protect passwords if the service is compromised, the implementation of the PRF is weak, or the key involved in the PRF is leaked. As a follow-up to Pythia, *partially oblivious commitments* (PO-COM) were proposed by Schneider [LES+ 2017]. Later on, Phoenix [SFS+ 2016] showed that the aforementioned scheme is vulnerable to offline attacks.

Pythia, PO-COM, and Phoenix are all based on elaborate cryptography for deploying services for hardening passwords. In contrast, in this vertical we follow a simpler approach for hardening passwords, without the need of an external service.

Finally, Password Authenticated Key Exchange (PAKE) [BPR 2000, BMM 1992, Wu 1998] can utilize cryptographic protocols that involve keys generated from passwords. Many of these protocols allow clients to prove knowledge of their passwords, without revealing them to servers. Instead, the server stores credentials that somehow embed information about the password, but not the password itself. Therefore, these systems focus on a different problem, namely, how to authenticate to servers without ever revealing the password to them.

#### 5.6.1.2 Unlinkability and minimal disclosure

In the context of minimum disclosure and unlinkability of user actions, a large body of work has been carried out over the last decades. In his seminal work, Chaum [Chaum 1981; Chaum 1985] introduced the concept of anonymous credential systems, which allow a user to obtain a certificate on her attributes, and later selectively reveal them to a relying party in such a way that different actions of a user cannot be linked without her explicit consent. This idea was later instantiated by Camenisch and Lysyanskaya [CL 2001, CL 2002], followed by a long series of work, including, e.g. [CL 2004; PZ 2013; RVH 2017]. In order to

overcome efficiency bottlenecks, especially on the-end user side, the concept of cloud-based anonymous credential systems has recently been introduced [KLS+ 2017; HK 2019]. The technical applicability and usability of anonymous credentials have been tested and evaluated in an ongoing series of European research projects, including FP6 PRIME<sup>231</sup>, FP7 PrimeLife<sup>232</sup>, FP7 ABC4Trust<sup>233</sup>, H2020 CREDENTIAL<sup>234</sup>, H2020 OLYMPUS<sup>235</sup>, or H2020 ARIES<sup>236</sup>, resulting in prototypical implementations with different maturity levels. Moreover, works like [BHR 2017] proposed a privacy-preserving and distributed solution for identity management and access control in an IoT environment.

One of the most relevant works on privacy-preserving attribute-based credentials, which was used in many of the projects mentioned in the previous paragraphs, is Idemix [CMS 2010]. While it has gained a lot of academic traction, the final adoption has been rather lacking. The main causes for this were its usability issues: the scheme is relatively slow, and its use caused many difficulties to end-users and developers. IRMA<sup>237</sup> applies Idemix with clear improvements in usability (except for the efficiency of the solution) but introduces the IRMA server as a central entity that can jeopardise user privacy (e.g. by learning all policies, and directly contributing to all interactions).

Some new works in the field of privacy Attribute-Based Credentials (p-ABC) have been published. P-ABCs are signed credentials that can be used to generate tokens where only a subset of attributes (or even partial information about them, like an integer being greater than a value) are revealed. The veracity of the tokens can be checked, but information is protected through zero-knowledge proofs, allowing unlinkability and minimal disclosure. [CDL 2020] introduces distributed p-ABCs based on multi-signatures (apart from more general group signatures), which are being considered for the distributed oblivious identity management system in the project pilots. Other notable works are [HP 2020], which presents aggregatable and *traceable* p-ABCs for accountability in case of credential abuse (using a tracing authority), and [Sanders 2020], which uses redactable signatures (starting from the PS scheme) to propose efficient p-ABCs.

Not much work on developing new p-ABC schemes can be found in the literature from the last year. However, there have been multiple works focusing on the application of p-ABCs for unlinkability and minimal disclosure. For instance, EL PASSO [ZKS+ 2021] proposes an interesting way of utilising p-ABCs for web-browser based authentication. Of high present relevance are applications of p-ABCs to achieve privacy by design in health passports (e.g. COVID green pass), such as [Frederiksen 2021]. Other common applications of credentials, such as privacy in DLT scenarios, are still trending. For instance, [Sarier 2021] explores the application of credentials with the addition of biometrics to ensure non-transferability. Issuer-hiding attribute-based credentials, allowing one to hide the precise issuer of a certificate, have been

---

<sup>231</sup> <https://cordis.europa.eu/project/rcn/71383/factsheet/en>

<sup>232</sup> <https://cordis.europa.eu/project/rcn/85453/en>

<sup>233</sup> <https://abc4trust.eu/>

<sup>234</sup> <https://credential.eu/>

<sup>235</sup> <https://olympus-project.eu/>

<sup>236</sup> <https://www.aries-project.eu/>

<sup>237</sup> <https://privacybydesign.foundation/irma-en/>

introduced by Bobolz et al [BEK+ 2021]. Efficient and practical schemes have also been suggested by Hanzlik and Slamanig [HS 2021].

### 5.6.1.3 Distributed oblivious identity management

Aggregatable and distributed credentials mentioned in the previous section (e.g. [CDL 2020]) can be building blocks for the distributed oblivious identity management, as once the user has her credential, she can create presentations that will be unlinkable both to other presentations and to the credential they come from (unless some mechanism is built-in for traceability, like a mandatory “key” attribute). Other cryptographic techniques like blind signatures [Chaum 1982] (combined with zero-knowledge proofs of knowledge to ensure veracity) or oblivious pseudorandom functions [FMI+ 2005] can be used to hide information from servers/issuers. Distributed variants of the latter are especially relevant to this challenge. Threshold oblivious pseudorandom functions were used in (PASTA) [AMM+ 2018] to obtain threshold oblivious password based SSO. The work by Baum et al. [BFH+ 2020] improved upon the PASTA approach to obtain a proactively secure SSO under universal composability, though under the constraint that the system is now fully distributed (as it is based on a distributed partially oblivious PRF).

For other publications more related to privacy-preserving identity management as whole, [BDM+ 2020] stands out as an evaluation of the result of a previous European project focused on an identity management framework (using Idemix credentials [CL 2001, CL 2002] as a privacy-enhancing technology). Also, closely related to the activities on this project, the publication [MBG+ 2020] describes a mature architecture of the OLYMPUS project, whose main goal is developing a distributed oblivious identity management system, which includes distributed p-ABCs as one of the complementary solutions for token generation.

In [MGB+ 2021], the extension of the infrastructure with a DLT and smart contracts for trusted public data sharing and auditing is recounted. For its part, [ZKS+ 2021] introduces EL PASSO, which enables single-sign-on capabilities (OIDC-like flow) with privacy-preserving properties based on p-ABCs (in particular, Pointcheval–Sanders signatures). The solution is presented as a kind of web-browser plugin, where an oblivious issuer (blind signatures) generates credentials that can then be used to authenticate against service providers. As caveats, the solution relies on a single IdP (so the solution is not distributed) and does not clarify how the infrastructure could be deployed in practice with guarantees of trust in issuers for users/service providers.

### 5.6.1.4 Privacy preservation in blockchain

Traditional identity management systems (IDM) adopt centralized models. These models are well known and present limitations and weaknesses when it comes to security, privacy, and scalability. In these centralized architectures, identity providers take an excessively powerful role when managing the identities.

Blockchain technology proposes an infrastructure that is no longer centralized and enables protection for the managed information. The immutability of data and transparency are interesting qualities for identity management. Blockchain is a very promising approach however, it has some challenges [BBC 2019]. Compliance with legal regulations (GDPR), scalability or privacy issues, which undermine user anonymity, confidentiality, and privacy control cannot be ignored.

Blockchain is gaining importance beyond cryptocurrencies. Proposed works included in [BLZ+ 2020] and [BBC 2019], apply blockchain to very diverse fields like health [HKK+ 2018] [KRAB+ 2018] which is particularly sensitive, smart cities [SMP 2017] or privacy management [WNR+ 2018] having a great potential for this technology. The features provided by Blockchain as the decentralization of the system, the operation without the need to trust third parties, the transparency it provides, and the simplification of multi-organization scenarios make it a technology to be considered when managing digital identity.

Nevertheless, decentralized approaches like the one shown by [MBG+ 2020] can potentially be combined with Blockchain/DLT technology bringing the advantages of both models while focusing on digital identity management.

During the last year, research on privacy-preserving identity management in blockchain has continued in force. The DID specification<sup>238</sup> is still being updated and maintained. Proposals like [SLC+ 2021] propose decentralised identification through pseudonyms, gaining unlinkability but making it difficult to ensure minimal disclosure when identities are composed of multiple attributes. Other proposals focus on credentials and zero-knowledge proofs to achieve privacy features. For instance, [Sarier 2021] is centred around zero-knowledge proofs from credentials, where non-transferability is tackled through biometrics. [MGB+ 2021] introduces a complete identity management infrastructure, including a distributed identity provider that generates p-ABCs, and smart contracts for auditability. Research related to revocation in self-sovereign identity management systems was performed by, among others, Abraham et al. [AKM+2021] and Helminger et al. [HKRW 2021].

In addition, alongside privacy and identity management approaches, research is also being developed to reduce the environmental impact of DLT-based technologies [BMZ 2018]. The most popular platforms (i.e. Bitcoin, Ethereum) are highly energy inefficient because of the proof-of-work based consensus algorithm. The new research approaches are moving away from this type of proof to implement others, such as proof-of-stake or proof-of-importance, which are more efficient. Our approach starts from the traditional proof-of-work, but the medium-term roadmap includes its replacement by the new and more efficient consensus algorithms.

#### 5.6.1.5 Password-less authentication

Nowadays an average person has 70-80 passwords according to a research conducted by NordPass, which offers password manager solutions [HSMC 2020]. To deal with all these accounts, users usually are taking actions that have serious consequences in the security of their accounts and the privacy of their data, e.g. use the same password in multiple accounts, use simple passwords, etc. The weaknesses and disadvantages of the traditional username-password paradigm have become obvious, thus, alternative authentication solutions, which will not rely on text-based passwords need to be employed by service providers. The technologies and standards in the field of password-less authentication are still limited. However, the latest standards for password-less authentication that have been developed by Fast Identity Online (FIDO) Alliance<sup>239</sup> are constantly gaining popularity. Recently the FIDO standard has been adopted by many big

---

<sup>238</sup> <https://www.w3.org/TR/did-core/>

<sup>239</sup> <https://fidoalliance.org/>

companies, like Google and Facebook. In particular, the FIDO standards are designed to support a variety of authenticators, like security keys, smartphone, fingerprint, handprint, voiceprint, eyeprint, faceprint and location. These standards referred to FIDO Universal 2nd Factor (U2F) [SBT+ 2015], the FIDO Universal Authentication Framework (UAF) [BHH 2013], and the FIDO2<sup>240</sup> that is developed jointly by FIDO Alliance and World Wide Consortium (W3C). The FIDO U2F augments the security of an existing authentication method by adding a second factor to user login. Usually, it is implemented together with traditional username-password authenticators, however, it can also be implemented together with other authenticators. The FIDO UAF involves two entities (i.e. client application & server) to perform the authentication using a challenge-response scheme. It supports multiple password-less authentication methods, and it offers strong authentication, due to its reliance on public key cryptography. Last but not least, FIDO2 is an extension of its predecessors U2F and UAF that not only offers the same high-security levels, but also extends their functionalities by deploying the WebAuthn protocol<sup>241</sup> and the Client-to-Authenticator-Protocol (CTAP2)<sup>242</sup> to authenticate a user in a browser application using a conforming cryptographic authenticator that can be external and roaming via NFC communication, Bluetooth or USB (e.g. security key or Android smartphone) or it can be internal (e.g. TPM, TEE, etc.). In contrast to its predecessors, FIDO2 supports single-factor authentication, two-factor authentication, as well as multifactor authentication. Moreover, OpenID Connect utilized the concept of identity token by building an authentication layer on top of OAuth2.0 [HH 2011]. When integrated with FIDO, OpenID Connect can support all the aforementioned password-less authentication methods.

Regarding the scientific efforts on password-less authentication, various ideas/solutions have been proposed. The authors of [ZFG 2014] presented an authentication solution named Loxin that exploits the push message services for mobile devices and enables users to access various services using online identities that they already own, such as email addresses, along with an interaction on their mobile devices (i.e. clicking on a notification). Loxin advantage is its resilience on man-in-the-middle and replay attacks. In [LSN+ 2020] the authors conducted a large-scale comparative user study of FIDO2 password-less authentication, and the results indicate that the users are willing to accept such password-less authentication over regular text-based passwords. A recent work from Papadamou et al. [PZC+ 2020] proposed the elimination of passwords and preserving privacy by deploying device-centric and attribute-based authentication. In [AWA+ 2020], the authors showed why the FIDO password-less authentication is more secure than the traditional password-based authentication by examining the attack surface. Their analysis concluded that indeed the FIDO password-less authentication is more secure than the password-based authentication because its attack surface is smaller. Connors and Zappala [CZ 2019] presented a certificate-based authentication method where the certificates of each client are managed by an authenticator. Their solution offers automatic registration and login, easy account recovery and privacy protection, however, it is a centralized solution as it is built on top of a CA.

During the last year, there have been several advances in the field of passwordless authentication, and especially concerning the FIDO protocol. [APX 2021] presented a comparison of the different FIDO protocols in terms of technical and security design and implementation, as well as an in-depth study on their adoption by different markets and business sectors. The authors also delve into possible drawbacks or

---

<sup>240</sup> <https://fidoalliance.org/fido2/>

<sup>241</sup> <https://fidoalliance.org/fido2/fido2-web-authentication-webauthn/>

<sup>242</sup> <https://fidoalliance.org/specifications/download/>

difficulties in the implementation of the FIDO protocols and elaborate on the outlook for future directions that the different versions of FIDO should aim for. [GPX 2021] introduced a web tool analyser of FIDO2/WebAuthn requests and responses that makes it easier for developers to comprehend how FIDO2 works, and helps penetration testers by editing the WebAuthn requests and responses and monitoring the responses of the application. [XSW+ 2021] proposed SSD, a trusted display of FIDO2 transaction messages, developing lightweight and trusted hardware without a trusted execution environment. The authors evaluated their solution in response to well-known attacks (XSS, implicit authentication attack, and mal-process occupying attack). An attack, named HIENA, was proposed in [JSS+ 2021] that targets passwordless and second factor authentication based on a “one-push” scheme.

#### 5.6.1.6 GDPR and eIDAS impact interoperability

European regulations on data protection and authentication are important aspects of providing identity management. Since the GDPR became applicable, there has been some work done to help explain all of its requirements and some tools that were introduced to help organizations perform the DPIA which is one of the more complex previously mentioned requirements. In the following we give a brief summary of the most prominent solutions in the field.

As for guidelines on GDPR compliance, there are a lot of them, but few go into any depth. The first and foremost crucial recommendations are from the EU’s body tasked with maintaining the consistent application of the GDPR rules in all Member States: the European Data Protection Board (EDPB)<sup>243</sup>. When looking at a specific problem on how to apply a given GDPR rule, this should be the first resource; however, for somebody who is interested in getting a walkthrough of the whole process of complying with the regulation, this is not a good source of information, as the guidelines, recommendations, and best practices given are very specific and cover only specific parts of the regulation. The other good resources for guidance are the national data protection agencies. Usually, each will have a webpage with the most common practices of applying GDPR in their own country, with the additional benefit of already taking into consideration any additional national/local legal requirement and/or recommendations<sup>244</sup>.

A special attention within the GDPR, has to be given to the Data Protection Impact Assessment (DPIA). There has already been some work done on providing a tool to assist with the DPIAs. There have been tools designed for general purpose (i.e. for anybody to use them in their scenario). The most notable of these are from the United Kingdom’s Information Commissioner’s Office [ICO], the of the European Union Agency for Cybersecurity (ENISA) (online tool<sup>245</sup>), and the French Commission Nationale de l’Informatique et des Libertés (CNIL) [CNIL 2021]. Other tools have also been developed and shared freely<sup>246,247</sup>. There have also been good examples of directions for the assessment of specific data processes, which can be adopted for other use cases.

---

<sup>243</sup> [https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices\\_en](https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en)

<sup>244</sup> [https://edpb.europa.eu/about-edpb/board/members\\_en](https://edpb.europa.eu/about-edpb/board/members_en)

<sup>245</sup> <https://www.enisa.europa.eu/risk-level-tool/>

<sup>246</sup> <https://github.com/simonarnell/GDPRDPIAT>

<sup>247</sup> <https://github.com/CSR-AIT/dpia-tool>

Examples are the templates for performing Data Protection Impact Assessment (DPIA) by the Edinburgh Business School [EBS 2018], the University of the West of England [UWE], or the Imperial College London [ICL], and the Code of Conduct and DPIA template by Family Links Network [FLN]. There have also been a few projects<sup>248,249</sup> funded specifically to create tools for the support of the DPIA process.

For more information and some differences between these tools, please refer to the D3.11 *Definition of Privacy by Design and Privacy Preserving Enablers*, section 3.1.1 *Data Protection Impact Assessment Templates* [Sforzin 2020].

#### 5.6.1.7 Identity Management Solutions for the IoT

Besides the generic privacy-preserving identity management solutions discussed above, over the last years a line of research specifically focusing on IoT devices has also started. A first requirements analysis and discussion of challenges in this context was carried out by Mahalle et al. [MBP+ 2010]. A series of frameworks for identity management in the IoT has subsequently been introduced, e.g. Horrow and Sardana [HS 2012], Fremantle et al. [FAK+ 2014], Nuss et al. [NPK 2018], or Lücking et al. [LFL+ 2020], among many others. While designed with fundamental privacy requirements in mind, most of these solutions do not give formal cryptographic privacy guarantees at a level that can be compared to the privacy-preserving identity management solutions discussed in Sections 5.6.1.2 and 5.6.1.3. On the other hand, many of the solutions there are not suited for the limitations and specific challenges of the IoT setting. Exceptions are, among others, the cloud-based schemes by Krenn et al. [KLS+ 2017] [HK 2019] and the framework defined by Bernal et al. [BHR 2017], which present relevant steps towards a fully privacy-respecting solution, also considering the specifics of the IoT environment. In addition, while not yet being fully practical on low-cost embedded devices, approaches like the recent work of Boneh et al. [BEF 2019], building privacy-preserving primitives (e.g. group signatures that are a building block of anonymous credential systems) from symmetric cryptographic primitives, might also be an interesting starting point for further research.

Moreover, in the last year, there appear several works related to IdM on IoT scenarios, most of them related to DLTs due to the usual decentralized and large-scale nature of these scenarios. [Bouras et al 2021] proposes a lightweight Blockchain-Based IdM approach by using a permissioned blockchain, which is better in terms of performance, privacy and trustiness because of its nature as an “invitation-only” DLT, and the use of smart contracts. In [VMA 2021], the authors work on an architecture for industrial Internet of Things (IoT) system, establishing distributed Identity and Access Management (IAM) using blockchain the communication layer. On a different note, the interest on Physically Unclonable Functions (PUF) to provide advanced security primitives in IoT (especially Industrial IoT) is rising [BCBMM 2021]. [PA 2021] establishes a distributed way (through cryptographic secret-sharing) of authentication based on PUFs to increase fidelity and security against attacks like curious intermediaries.

---

<sup>248</sup> <https://localdigital.gov.uk/funded-project/digital-data-protection-impact-assessment-dpia-tool/>

<sup>249</sup> <https://www.dsfa.eu/index.php/en/home-en/>

## 5.6.2 SWOT Analysis



Figure 9: Privacy-Preserving Identity Management SWOT Summary

In the current ecosystem, online interaction has reached a global scope, both in terms of “geography” (international connections) and “life dimensions”. Hence, security and privacy of online identity management have become a great concern. A SWOT (Strength, Weakness, Opportunity, and Threat) analysis is conducted to understand EU’s readiness to face the threats involved in identity management and become a leader in this area. A summary of the supply chain SWOT analysis is presented in Figure 9, while a more detailed explanation of the results comes in the following.

### 5.6.2.1 Strengths

- The **EU has a strong position on identity management and the use of personal data**. Over the last few years, many projects (such as H2020 ABC4Trust<sup>250</sup>, H2020 ARIES<sup>251</sup>, H2020

<sup>250</sup> <https://www.abc4trust.eu/>

<sup>251</sup> <https://www.aries-project.eu/>

OLYMPUS<sup>252</sup>) have been developed with the main aim of improving the protection of its citizens' personal data. Moreover, **European legislative initiatives such as the GDPR provide useful legal tools for the technical development of data protection.**

- Another strength of the EU is also the **strong data protection, privacy and cross-border operability regulations that are present within the EU.** These ensure the accountability of anybody mistreating vital and personal data, while assuring EU citizens of the responsible management of their private data.
- **Companies adapting the technology benefit from compliance with legal regulations** such as the GDPR, as anonymous credentials are an important technology for technically enforcing the data minimization principle.
- With the existing research base, the EU can improve data protection and enforce minimum standards by strengthening the protection of its citizens. The **ppIdM research will protect against the most important threats to privacy, data and identity theft** that have increased their impact in recent years, as a result of the rise of internet services that have put the focus on user data as their main asset.
- Reduced risk (in terms of fees, reputation, etc.) **in case of data breaches, as due to the data minimization features of credential systems, less sensitive data may be leaked to an adversary.**

#### 5.6.2.2 Weaknesses

- **Identity management systems have many applications.** Each of them uses **specific and original solutions, leaving aside standardisation,** which makes the adoption of these technologies difficult. It is necessary to address the problem from a homogeneous platform that allows the various actors involved to make use of these solutions in a simple way.
- **Another problem comes from the “attitude” of users and service providers.** Although advances have been made in both fields, **it is necessary to instil in users the great importance of their privacy in digital transactions and how it may be jeopardized/protected,** and strictly regulate so services do not base their business on user data with no regard to privacy.
- While strong regulation of personal data protection, privacy and cross-border operability is one of the strengths, the regulations also cause some adverse effects. **Strong regulation can introduce the problem of additional work for companies doing business in the EU (as compared with the rest of the world) and a higher entry cost or upfront cost, which is especially detrimental for new businesses.** This also lowers the chances of successful solutions being created by EU-based organizations, as they are often launched in a local region and spread across the world after becoming popular in that single part of the world. For EU-based organizations this involves much more work than launching a solution in other parts of the world. The lack of support (technical, financial, etc.) for organizations, especially new/small ones, in their efforts to comply with the regulations can, therefore, become a significant weakness.
- **Existing non-privacy preserving solutions are often easier to implement for a developer** computationally less demanding; given that security and privacy are non-tangible, and (hardware)

---

<sup>252</sup> <https://olympus-project.eu/>

requirements are higher for privacy-preserving solutions, providers may be reluctant to invest the necessary costs.

### 5.6.2.3 Opportunities

- There are opportunities **to protect users' privacy more effectively by reducing the control that major identity providers have over their users and by providing better tools to manage their personal information.**
- **It should be possible to create an EU-based independent identity management service**, which will be available for other applications and services to use. This would ensure that **directly identifiable information of individuals is kept securely, following all the EU regulation and best standards/practice.** To put it differently, the EU could provide for its citizens a hub for authentication, which they could then use to access all other services.
- **Technology has improved significantly over the last few years** (e.g. regarding efficiency), so it might be worth pushing for the **next generation of digital identities to be rolled out in member states.**
- Technologies and (importantly) dissemination to increase people's trust in the solutions can be applied to **address challenges and people's concerns about identity management-related solutions to large-scale and high-publicity issues.** A clear example of this is the impact of the COVID pandemic, where solutions to demonstrate immunity/testing results are needed (for travel, recreational activities, etc.) and raise legitimate concerns about privacy and citizen's rights.

### 5.6.2.4 Threats

- There are **other solutions on the market that are widespread among users**, despite being much less respectful of personal data privacy. Although a solution derived from research would be technically better, if we do not manage to convince users we will not achieve good adoption. Moreover, companies that control these solutions will fight to maintain control over users' private data, since it is their main source of income today.
- Another potential threat comes from **the "volatility" of regulation**, specifically GDPR and eIDAS. These regulations **might be subject to change over time depending on multiple factors.** This most affects the facet of this vertical that directly deals with these regulations to generate guidelines, but it is relevant for the general IdM aspects too, so continuous monitoring and support will be necessary.

## 5.6.3 European Digital Sovereignty

There is a growing concern that the citizens, businesses and Member States of the European Union (EU) are gradually losing control over their data, over their capacity for innovation, and over their ability to shape and enforce legislation in the digital environment. Against this background, support has been growing for a new policy approach designed to enhance Europe's strategic autonomy in the digital field.

Strong concerns have been raised over the economic and social influence of non-EU technology companies, which threatens EU citizens' control over their personal data, and constrains both the growth of EU high-technology companies and the ability of national and EU rule-makers to enforce their laws. Digital sovereignty refers to Europe's ability to act independently in the digital world and should be understood in

terms of both protective mechanisms and offensive tools to foster digital innovation (including in cooperation with non-EU companies).

The EU has created several instruments, such as the *Horizon 2020* research programme, and has adopted very stringent regulations for privacy and data protection, with the *General Data Protection Regulation (GDPR)* at its centre. The introduction of protective rights, such as the “right to be forgotten”, enhance individuals’ control of their own data. Furthermore, the Commission has set out a strategy for promoting international data protection standards. The EU is seen as a standard-setter in privacy and data protection, with various countries having incorporated GDPR provisions into their national legislation and some multinationals having opted to adopt GDPR as their global standard of operation.

The ppIdM research will contribute to this concern by providing better privacy management tools to its users, improving interoperability between EU members and effectively implementing directives like the GDPR. Furthermore, the analysis of the impact of GDPR and eIDAS (a key regulation for interoperability of digital identity in EU) will contribute to an improvement of the bases that govern the research and implementation of identity management tools within the EU.

Currently, most of the largest single sign-on providers (also the ones the typical user would most often use) are owned and operated by foreign companies. Development of this sector (in research and practice) would reduce this dependency for typical users and make it more likely for the related data to be stored in the EU.

#### 5.6.4 COVID-19 and Public Health Dimension

The COVID-19 pandemic has highlighted the extreme need to respect and protect users’ personal data. In the context of a health alert, numerous applications have emerged with the aim of tracing infections and obtaining information on the incidence of the virus. The protection of personal data becomes vitally important in this scenario.

The European Commission has recommended a common EU approach towards contact-tracing apps, which are designed to warn people if they have been in contact with an infected person. In a resolution<sup>253</sup> adopted on 17 April and during a plenary debate on 14 May, the European Parliament stressed that any digital measures against the pandemic must be in full compliance with data protection and privacy legislation.

The use of these apps and data might prove to be effective, but they could also expose sensitive user data, such as health and location. In this sense, ppIdM technologies can help users control the use of their personal data, while improving privacy in COVID-19 tracking apps. Besides, the increased use of digital services during the COVID-19 pandemic has also increased the amount of personal (meta-)data shared with service providers. Thus, reducing the privacy of every single online interaction is more important than ever.

Another consequence of the pandemic has been the great surge in the usage of digital entertainment (streaming, games, social media, etc.), even by people who were not used to this kind of platform before. As online activity rises, so does the potential risk and harm of privacy breaches and behaviour tracking. The

---

<sup>253</sup> ([https://www.europarl.europa.eu/doceo/document/TA-9-2020-0054\\_EN.pdf](https://www.europarl.europa.eu/doceo/document/TA-9-2020-0054_EN.pdf))

ppIdM technologies envisioned in this project can help against these issues, allowing users to enjoy those digital services without great concern about their privacy.

Regarding the public health dimension in general, many points related to COVID still apply. Other epidemic/pandemic situations (sadly predicted as impending by numerous scientists) could require similar responses in terms of identification. Experience gained from this pandemic and improvements in ppIdM solutions can be key for a better response that reduces the impact of future pandemics. Even in more mundane situations, such as the monitoring and treatment of patients (e.g. the elderly or diabetics) or research studies (e.g. obtaining statistics about some disease), ensuring that privacy is assured when managing people's health and identity data is critical.

In general, any situation that entails the management of user data within the public health system will be a potential application for ppIdM. The main example is the management of patients' health records, which may be needed in their place of origin, but also in any other health installation of the country and even other institutions (e.g. government or even private organisations that offer benefits tied to health conditions). In this case, ppIdM will be an asset for allowing this data sharing while ensuring that the patient's preferences regarding privacy are fulfilled. It can also act as an enabler of the whole process, as a set of tools to be used by the necessary access-control mechanisms.

### 5.6.5 Green Deal and Climate Change

While the relationship between ppIdM and the European Green Deal is not as direct as for other areas, it will still be a necessary resource for its completion. The reason is that other key components for the plan, such as Smart Cities, will need tools to provide secure authentication and authorization mechanisms while complying with regulations like GDPR that aim to protect user privacy.

Further, DLTs are rising in popularity for improving identity management solutions. While the properties of DLTs make them desirable for ensuring transparency, auditability and decentralisation, which are useful for the completion of the Green Deal, there are some concerns regarding their usage. Numerous studies have shown the impact of blockchain-based solutions in terms of energy consumption, such as the reports on Bitcoin's network high energy requirements, greater than countries such as Argentina. Another topic related to the same root problem is the high demand for computing elements (i.e. graphics cards), which has sometimes collapsed the market of these products (exacerbated by the current supply issues). These drawbacks need to be solved through further research, so that DLTs can actually be a feasible alternative for achieving privacy-preserving identity management. For instance, research on consensus algorithms with approaches differing from "proof of work" (such as "proof of stake", or "proof of importance"), which is one of the main reasons for the high energy consumption of many blockchain deployments, will be key in reducing the efficiency issues of DLTs and ensuring the feasibility of solutions based upon them.

This vertical has no direct relationship with the climate change dimension, except for the comments related to energy consumption described in the previous section.

## 5.6.6 Impact on Democracy

The EU is governed by three democratic principles of equality, participation and representation. Under equality, all citizens must be treated fairly and equally; this includes affording everybody the same options, opportunities, services, etc., that the EU provides for its citizens. Participation is about communication between the EU and its citizens. It ensures citizens have the right to participate in the decision making and are fully informed of any activities of the EU. In modern times both equality and participation are greatly aided by and reliant on information technology. An EU-wide single sign-on system would provide everybody with the same access options to the EU's services, opportunities and information (a.k.a. e-governance). A good example of this is the current Digital Green Certificate to facilitate safe free movement within the EU during the COVID-19 pandemic. There is no doubt this is a good solution that allows for the harmonisation of proving an individual's immunisation against the virus. At the same time, there is a large amount of confusion among citizens about what the Green Certificate actually is, or rather if the certificates issued by their national institutions meet the criteria.

If the certificates were issued based on universal EU authentication, there would be no doubt about it. Privacy-preserving identity management extends the options to use the same system for other non-EU services and even gives citizens the possibility of potentially using the same system for voting in elections.

This brings us to the third democratic principle: representation. In addition to the Member State's elections, the members of the European Parliament are elected directly by the citizens. In the effort to enable inclusive, credible and transparent elections while trying to increase voter turnout, serious considerations have been given to electronic voting over the internet. However, Internet e-voting is very rare, primarily because of the issues related to the possibilities for exploitation, trust in the technology, and the scope of consequences a successful attack on the system would have. While ppIdM cannot solve all of these problems, it can help alleviate at least some of them, such as validating a citizen's right to vote in a privacy-preserving manner, or (in combination with related privacy-enhancing technologies) ensuring that only a single vote is cast per voter in the final vote count.

Summarising, ensuring that citizens can manage their digital identities and preserve their privacy in digital interactions is fundamental for civil liberties and democracy (whether the PETs are directly applied, e.g. for a voting system, or are simply a tool for helping citizens in their interactions). However, potential issues may arise from anonymity in digital interactions: for example, potentially enabling the perpetrators of hacktivism, terrorism or disinformation to be immune to the consequences of their actions in the digital world.

## 5.6.7 Contributions to the EU CyberSecurity Strategy for the Digital Decade

### 5.6.7.1 Resilient infrastructure and critical services

The preservation of privacy is the main objective of this vertical. It is a fundamental stride towards strengthening the resilience of democratic processes and institutions. In addition, identity management through privacy-preserving techniques can be an enabler for other critical services, e.g. by reinforcing supply chains, and therefore results in this field can contribute to improving the resilience of the entire systems in which services take place.

### **5.6.7.2 Building a European Cyber Shield**

While this vertical may not have a direct impact, some kind of identity management solution is needed for trusted data sharing (and specifically sharing of cyber-threat data), so the results on privacy-preserving identity management may enable future developments in this scope.

### **5.6.7.3 An ultra-secure communication infrastructure**

Again, this vertical can indirectly impact the development of ultra-secure communication infrastructures as the results for identity management can be enablers for architectures or components that are useful to this end. This is because strong authentication mechanisms are fundamental for secure communication, and the technologies developed in this vertical provide high authenticity guarantees on the disclosed user data.

### **5.6.7.4 Securing the next generation of broadband mobile networks**

Solutions for secure and privacy-preserving identity management are a building block for backend infrastructures (e.g. for access control, monitoring of entities, etc.) that will enable secure next generation broadband mobile networks.

### **5.6.7.5 An Internet of Secure Things**

Security and privacy-preservation in identity management are necessary pillars for a secure Internet of things landscape. The results of this vertical (specifically Challenge 7, although others can be a departure point for future developments in this line) are relevant for this evolution.

### **5.6.7.6 Greater global Internet security**

This vertical does not directly contribute to this dimension.

### **5.6.7.7 A reinforced presence in the technology supply chain**

This vertical does not directly contribute to this dimension.

### **5.6.7.8 A cyber-skilled EU workforce**

This vertical does not directly contribute to this dimension.

### **5.6.7.9 EU leadership on standards, norms and frameworks in cyberspace**

Many international standardisation efforts for identity management technologies, and specifically for privacy-preservation, are being energetically (co-)developed by European researchers and organisations. Examples include privacy preservation in W3C's Verifiable Credentials specification, as well as novel and upcoming international standards (e.g. ISO/IEC 27551 for attribute-based authentication mechanisms, ISO/IEC 20008-2 for group signatures, ISO/IEC 23264-1/2 for redactable signatures as building blocks for pABCs, or ISO/IEC 20009-3 for anonymous entity authentication).

### **5.6.7.10 Cooperation with partners and the multi-stakeholder community**

Active cooperation with partners makes it possible to establish relationships on which to base the proposals made, as well as their integration in pilots or proofs of concept that may subsequently, in the medium or long term, give rise to commercial products that implement the innovative solutions obtained.

### 5.6.7.11 Strengthening global capacities to increase global resilience

Improving digital identity management processes with privacy-preserving features is intended to promote a general framework for engagement that can comprehensively improve the way in which citizens' digital identities are managed all over the world, even in cross-border scenarios.

### 5.6.8 Sector-specific Dimensions

Although there are scenarios where privacy protection through technical approaches is more relevant (e.g., the use of boarding passes to purchase restricted goods like alcohol) in scenarios where there are numerous untrusted services, i.e., smart cities, ppIdM tools are a good tool for the protection of users' digital identity. This project proposes strong collaboration between ppIdM and smart cities verticals where the results obtained in the case of digital identity management through privacy-preserving processes will lead to components and pilots in the case of the smart cities scenario. This is intended to substantially improve privacy qualities in the context of smart cities so that even in a context where there is low trust in services, users are not pushed to leak more information than necessary and avoid compromising their personal data. In that sense, any user will be able to operate with a certain level of security and privacy, even if they are unaware of the trust level and leading to a Smart city scenario with protection by design.

### 5.6.9 Summary of the dimensions and impact on the Roadmap

The previous sections give an overview of the different dimensions and how they interact with this vertical of privacy-preserving identity management. As a main recurring idea, the high digitalisation of all societal aspects demands that identity management solutions are improved to tackle trust, privacy and security challenges. Even when identity management is not strictly related to a specific topic, it will still be a necessary tool for the backbone of the digital solutions that are applied. Thus, the focus of the roadmaps defined in this project has been on the development and evolution of identity management tools that ensure security and trust in authentications while empowering users' control over their data, as well as solutions for enabling the application of Europe's regulations. Furthermore, specific goals and focus points within the developed roadmaps (standardisation of PETs, compliance with regulations, current developments such as health passports, etc.) have been derived from the ideas identified in the analysis of the dimensions.

### 5.6.10 Challenge 1: System-based credential hardening

The identity of a user is bound internally in the system using some sort of credentials, so that the system can authenticate the given identity in the future. Beyond protecting the data that is associated with the identity, the system also needs to protect this identity binding (i.e. the user's credentials). Nowadays, this binding is often associated with a text-based password. In particular, the system stores the cryptographic hash of a secret word for each identity, in order to be able to verify it. More elaborate bindings have been proposed in the form of graphical passwords or multi-token ones. No matter the technique used, it is important that, during a system compromise, credentials should be strongly protected. Otherwise, easily reusing stolen credentials puts at stake the identity of the user and all data associated with it.

#### Relevant Research Goals

- *Making cracking hard, by means of computational effort* by using several layers of encryption and hashing of a given password, so that cracking a leaked password may require additional information provided by a different entity.

- *Storing (protected) non-text-based credentials in a database*, since it is difficult to process non-textual data using cryptographic primitives, such as cryptographic hashing.

#### JRC Cybersecurity Domain:

- Identity management
  - Privacy and identity management;
  - Identity management quality assurance.

#### JRC Sectorial Dimensions:

- Safety and Security
- Digital Services and Platforms

#### JRC Applications and Technologies Dimensions:

- Information systems
- Critical infrastructures Protection
- Disaster resilience and crisis management

### 5.6.11 Challenge 2: Unlinkability and minimal disclosure

Access to online services requires user identification and, in many cases, verification of certain attributes, such as age or country of residence. However, in order to prove the veracity of this kind of attributes users usually have to present extra information, such as credit card information, electronic IDs (that contain full name, nationality, etc.) or full address. In addition, service providers can collude to track users and share their data. In this scenario, users' privacy is severely compromised.

#### Relevant Research Goals

- *Development of an Identity Management System that provides minimal disclosure and unlinkability* between service providers. Here, minimal disclosure means that using this system it is possible to prove that the user meets a specific requirement, for example being over 18 years old, while not revealing any other information. In this case, unlinkability of the presented information becomes a necessary property, as revealing even the minimal information required to perform different transactions would lead to full disclosure when collaborating service providers share their common data about the user.
- Investigate the issues that caused previous academic solutions (e.g. Idemix, IRMA) that provide these properties have to have poor adoption and aim to address them when developing the identity management system.
- *Adopt and integrate existing technologies*, with the support of advanced and innovative techniques like privacy attribute-based credentials

#### JRC Cybersecurity Domains:

- Identity management
  - Identity and attribute management models, frameworks, applications, technologies, and tools;
  - Privacy and identity management.
- Data security and privacy

- Anonymity, pseudonymity, unlinkability, undetectability, or unobservability;
- Privacy Enhancing Technologies.

#### JRC Sectorial Dimensions:

- Safety and Security
- Digital Services and Platforms

#### JRC Technologies and Use Cases Dimensions:

- Information systems
- Critical infrastructures Protection
- Disaster resilience and crisis management

### 5.6.12 Challenge 3: Distributed oblivious identity management

Even though unlinkability across multiple service providers could be accomplished using a single identity provider, this is not enough to protect users' privacy. Indeed, an IdP that generates tokens to prove users' identities for their online and offline transactions can track said users' activity, learning which services they interact with and when these interactions occur. Moreover, here arises the fundamental requirement of maintaining the same level of security as in the single IdP case. In particular, avoiding malicious user identity forgery for transactions becomes challenging, as the IdPs do not have information about the relying party involved in the process.

#### Relevant Research Goals

- ***Development of a distributed oblivious identity management system*** Such a system may rely on distributed cryptographic techniques to split the role of the online IdP between multiple authorities, so that no single authority can impersonate or track its users. In this case, tokens could be generated using threshold signatures, where any subset consisting of a certain threshold  $t$  out of the  $n$  authorities must collaborate to construct a valid signature, but a subset of fewer than  $t$  authorities cannot produce a valid one.
- ***Ensuring transparency in the change to distributed issuance*** to relying parties or that the overhead of using a distributed approach (complexity of cryptographic tools, communication needs, etc.) is not too high
- **Interoperability, simplicity and user-friendliness.** Even if the system is based on complex privacy-preserving techniques, it should remain user-friendly and as simple as possible. Interoperability with other (existing) approaches is also key to encourage adoption of such a system. These characteristics are challenging to achieve and have been great detriments to previous similar proposals.

#### JRC Cybersecurity Domain:

- Identity management
  - Identity and attribute management models, frameworks, applications, technologies, and tools;
  - Protocols and frameworks for authentication, authorization, and rights management;
- Cryptology
  - Secure multi-party computation;
  - Crypto material management.
- Network and distributed systems

- Distributed systems security;
- Protocols and frameworks for secure distributed computing;
- Privacy-friendly communication architectures and services.

#### JRC Sectorial Dimensions:

- Safety and Security
- Digital Services and Platforms

#### JRC Technologies and Use Cases Dimensions:

- Information systems
- Critical infrastructures Protection
- Disaster resilience and crisis management
- Blockchain and Distributed Ledger Technology (DLT)

### 5.6.13 Challenge 4: Privacy preservation in blockchain

Blockchains offer a decentralized, immutable and verifiable ledger that can record transactions of digital assets, provoking a radical change in several scenarios, such as smart cities, eHealth or eGovernment. However, blockchains are subject to different scalability, security and potential privacy issues, such as transaction linkability, on-chain data privacy, or compliance with privacy regulations (e.g. GDPR). In these scenarios, the people or devices involved in the transactions require the handling of their sensitive information in a privacy-preserving manner, while maintaining high reliability and data provenance. Moreover, for the devices involved, the anonymous authentication and the management of digital identities that are linked to a user, also make the privacy-preserving scenario a necessity. In blockchain scenarios, there is a large volume of information to handle. This information is introduced continuously and some of it could be highly sensitive, even without user or device awareness. For this reason, privacy-preserving approaches are needed while maintaining the capacity of unveiling the real identity of the owner associated with the exchanged data when the inspection grounds are met (e.g. identity theft or associated crimes).

#### Relevant Research Goals

#### Relevant Research Goals

- ***Investigate, integrate and adapt privacy-preserving solutions in blockchains***; privacy-preserving solutions, such as anonymous credentials systems (e.g. Idemix) in blockchains (e.g. Hyperledger), following a self-sovereign identity management approach more concretely, allowing for the possibility of using non-interactive zero knowledge proofs (NI-ZKP). To this end, it is envisaged that the outcomes from the Decentralized Identity Foundation (DIF) will be used as a baseline.
- ***Consider the efficiency issues of blockchain technologies*** and, specifically, the impact of consensus algorithms like proof of work, proof of stake and proof of importance on the feasibility of our solutions.

#### JRC Cybersecurity Domain:

- Identity Management
  - Identity and attribute management models, frameworks, applications, technologies, and tools

- Protocols and frameworks for authentication, authorization, and rights management;
- Privacy and identity management;
- Legal aspects of identity management.
- Cryptology
  - Secure multi-party computation;
- Data Security and Privacy
  - Design, implementation, and operation of data management systems that include security and privacy functions;
  - Anonymity, pseudonymity, unlinkability, undetectability, or unobservability.
- Network and Distributed Systems
  - Distributed systems security;
  - Secure system interconnection;
  - Privacy-friendly communication architectures and services.

#### JRC Sectorial Dimensions:

- Safety and Security
- Digital Services and Platforms

#### JRC Technologies and Use Cases Dimensions:

- Information systems
- Critical infrastructures Protection
- Disaster resilience and crisis management
- Blockchain and Distributed Ledger Technology (DLT)

#### 5.6.14 Challenge 5: Password-less authentication

Most web applications have authentication process that rely on the password paradigm. It is evident that a password can be considered secure when it contains 20 characters or more, is complex (is comprised of alphanumeric characters, symbols and non-dictionary words), is only stored in the brain of the user, is used only in one application and is changed frequently. As the number of accounts each user maintains has greatly increased in the last few years, users are having a hard time memorizing and managing all these passwords. To solve this password overload problem, users have come up with solutions that directly affect the security of their accounts and the privacy of their data; they either simplify their passwords to be easy to remember, or reuse the same password on different services, or store their passwords in a “secure” place, on paper or using a password manager. At the same time, passwords are targets of multiple attacks, as they can be leaked, key-logged, replayed, eavesdropped, brute-force decoded and phished.

#### Relevant Research Goals

- ***Development of password-less authentication solution***; in this context, the need to employ a secure and user-friendly password-less authentication solution has emerged. To be widely used, the solution should be easily adoptable by both end-users and service providers, as well as allowing integration with privacy-preserving identity management solutions, such as Idemix.

#### JRC Cybersecurity Domain:

- Identity and Access Management
  - Identity and attribute management models, frameworks, applications, technologies, and tools;

- Protocols and frameworks for authentication, authorization, and rights management;
- Authentication/Access Control Technologies (biometrics);
- Privacy and identity management;
- Identity management quality assurance.
- Human Aspects
  - Enhancing risk perception;
  - Usability;
  - Automating security functionality,
  - Privacy concerns, behaviours, and practices.

#### **JRC Sectorial Dimensions:**

- Safety and Security
- Digital Services and Platforms

#### **JRC Technologies and Use Cases Dimensions:**

- Information systems
- Critical infrastructures Protection
- Disaster resilience and crisis management
- Blockchain and Distributed Ledger Technology (DLT)
- Human Machine Interface

### **5.6.15 Challenge 6: GDPR and eIDAS impact on Identity Management**

Like any other legislation, and even more so as the GDPR is meant to be a framework, the nuances of the regulation are often complex. This stems from the differences how the holders of data interpret the regulation and how the European courts interpret it, and what each of the parties considers appropriate ways of implementing the given regulation. This in connection with assuring the compliance with the regulation brings many challenges.

The regulation was designed to give the citizens of the EU and EEA greater control over their personal data and ensure that their information is being adequately protected. For any entity that processes personal data and does not comply with the regulation, the GDPR stipulates harsh fines. According to the GDPR, personal data is any information related to a person such as a name, a photo, an email address, a computer IP address etc. Identity management, therefore by default, contains personal data.

Processing of personal data is considered lawful if the data subject has given consent, the processing is necessary for the performance of a contract, which the subject is a party in, the processing is necessary for compliance with a legal obligation, the processing is necessary for the protection of vital interests of a natural person (the data owner or somebody else), the processing is necessary for the execution of a task in public interest or the processing is necessary for the purpose of a legitimate interest pursued by a controller or a third party. When providing privacy-preserving identity management as a service, the provider is considered a third party, and therefore needs to have appropriate contracts establishing the relationship between the controller and processor. In such a case, the controller will most likely wish to ensure the processor is fully compliant with all GDPR requirements.

Also, under the GDPR both the data controller and processor shall implement appropriate technical and organizational measures (as described in deliverable 4.2, by the task 2 in work package 4) to ensure a level of security appropriate to the risk. Management of risk also brings into consideration the Data Protection Impact Assessment (DPIA). DPIA is a legal requirement under the GDPR when the processing of data is likely to result in a high risk to the data owners. It is a process designed to help identify and minimize data protection risks. It increases the awareness of issues related to privacy and data protection within an organization. This provision of the GDPR could be very important for an identity management system, especially when this solution is used to provide management for multiple services. DPIA is essentially legally required (for certain situations) but more limited form of risk management.

GDPR requires that consent must be freely given, specific, informed and unambiguous. This can have major implications for an identity and authorization management system, as most users consent, especially for the online services, is managed through their user profiles. The identity management platform should provide a record of consent given, the ability for data subjects to withdraw any or all consents given and an audit functionality of all consents given and revoked. Identity management can manage identities for different actors. Given different access right and data that is stored about different users, it could be a challenge for an identity management system to ensure that transparency and other data owners' rights (right to erasure, restricted processing etc.) are provided to natural persons as the GDPR demands.

Each of the member states was required to implement the EU Electronic Signature Directive into their national law. This caused two undesirable outcomes. In some cases, the local legislation was not produced in time to support the rollout of the eIDAS. The freedom the regulation left the member states when designing their own systems, has also led to problems. Different member states have proposed and implemented different solutions that are not necessarily compatible between member states, in turn defeating the principal idea behind the eIDAS. Further, member states were left with the freedom to regulate their own measures in other areas of electronic commerce. This is leading to the position where other regulations come into conflict with the eIDAS regulation. This is blocking further harmonization of the Single European Market.

Establishing an efficient and usable infrastructure of electronic identifications and trust services across the member states demands adaptation and integration of many systems and legislation of the members, that were originally established and run by different entities. Each of the Member States of the EU was required to implement the EU Electronic Signature Directive into their national law. However, the Electronic Identification and Trust Services Regulation applies directly to every EU Member State. This means that many laws, if not every law, might need to be amended in due course. Further many businesses can't properly distinguish between trust levels and don't understand which one they should be using.

When developing a new (privacy-preserving) identity management system, the requirements of the eIDAS regulation should be carefully considered and implemented into the final solution, especially if the goal of the system is to be used on a large scale and across member states.

### Relevant Research Goals

- **Establish GDPR guidelines.** The resulting guidelines will collect and present in a simple and understandable way the specific points of the GDPR regulation and provide best practices. GDPR

requirements will be presented through examination of the GDPR privacy principles and through a guided process of performing a Data Protection Impact Assessment (DPIA).

- **Analyse interoperability and cross-border compliance of the eIDAS between different countries.** The main objective of this work is to find discrepancies between member states and possibly identify security shortcomings of a given authentication implementation. This could be beneficial for the field of identity management to ensure compliance with the eIDAS and avoid bad practices.

#### JRC Cybersecurity Domain:

- Identity and Access Management
  - Privacy and identity management;
  - Identity management quality assurance.
- Legal Aspects

Cybersecurity regulation analysis and design.

#### 5.6.16 Challenge 7: Identity Management Solutions for the IoT

Over the last two decades, a variety of privacy-preserving protocols for identity management have been developed and tested in different scenarios and domains. However, while achieving high privacy guarantees, virtually all existing solutions require computationally heavy computations on both, the user's as well as the verifier's side.

Similarly, over the last years, the number of connected devices and sensors has significantly increased, ranging from connected vehicles over wearables to medical devices or household devices. All these devices may perform authentications on behalf of the user, and thus their cryptographic functionalities directly impact their owner's privacy. However, due to cost, bandwidth, or energy constraints, many of these IoT devices are only able to perform a limited amount of computations.

To close this gap between high computational costs and available capabilities, it is necessary to develop privacy-preserving mechanisms which fully take into consideration the resource-asymmetry between the authenticating device and the verifier.

#### Relevant Research Goals

- **Resource-efficient identity management solutions.** Already in the design phase of identity management solutions computational or bandwidth constraints of the authenticating or the verifying parties need to be considered. The mechanisms then need to respect these constraints by minimizing the costs on the limited party's side.
- **Outsourcing of privacy-preserving identity management.** To overcome the described challenge, computationally expensive parts of the computation can be delegated to a semi-trusted authentication provider. The ambition is to minimize the necessary trust assumptions to this provider, also regarding meta data privacy, and to avoid a single point of failure.

#### JRC Cybersecurity Domain:

- Identity and Access Management

- Privacy and identity management;
- Identity management quality assurance.
- Data Security and Privacy
  - Anonymity, pseudonymity, unlinkability, undetectability, or unobservability
  - Privacy Enhancing Technologies (PET)

#### **JRC Sectorial Dimensions:**

- Safety and Security

#### **JRC Technologies and Use Cases Dimensions:**

- Internet of Things, embedded systems, pervasive systems
- Mobile devices

## **5.7 Mapping of the Challenges to the Big Picture**

Performing the identity management described in Section 5.1 in a privacy-preserving manner is a non-trivial subject. The actors with which users have to interact, that is, issuers and service providers, can become sources of privacy breaches willingly (because of financial interest) or not. During authentication, more information than intended by the user may be revealed to the service provider, or the information revealed to multiple service providers may be pooled to create a more complete picture of the user identity than expected (challenge 2). Also, an issuer becomes a single point of failure. A malicious or compromised issuer can track user activity and may lead to breaches of privacy (identity data is revealed) or even to identity theft or forgery (challenge 3). Lastly, it is necessary (and/or desirable) to conform to existing regulations regarding privacy while keeping in mind the possible interoperability issues (challenge 6).

However, protecting the user from the other malicious (or compromised) actors is not the only challenging matter. Other risks come from the software tools that are used or the possible misuse by the user himself. For example, as mentioned before, the most widespread method for authentication is the use of username plus password. While the method itself can be secure, in practice it leads to possible breaches because of weak or reused passwords and offline attacks (challenge 5). Also, when cryptographic materials like certificates or credentials are involved, they become assets that must be protected (e.g. a software-based wallet in the user device) and put the user identity at risk (challenge 1). Lastly, as new trends like the use of blockchain appear to improve the landscape of identity management, their compatibility with the existing scenarios and privacy-enhancing tools has to be assured (challenge 4).

## **5.8 Methods, Mechanisms, and Tools**

This section presents the mechanisms and tools needed to address the challenges described above. It also indicates which of these are being developed in WP3 and what additional methods need to be developed.

### **5.8.1 System-based credential hardening**

Currently, the most widely used form for protecting credentials is to store only the cryptographic digest of a “salted” credential. In other words, the system concatenates a random token to a text-based password, computes the cryptographic hash and stores it in a database. The plain password is eliminated. If the database is leaked, the attacker needs to crack the cryptographic hashes, which can sometimes be fairly easy, if they are based on weak passwords.

Further cryptographic techniques should be realized for: (a) making cracking hard, by means of computational effort, and (b) storing (protected) non-text-based credentials in a database. For (a) there are

currently proposals for advanced cryptographic services that use several layers of encryption and hashing of a given password, so that cracking a leaked password requires additional information provided by the cryptographic service. Nevertheless, additional research should be invested in making this domain more mature. For (b) little research has yet been done, since it is difficult to process non-textual data using cryptographic primitives, such as cryptographic hashing.

### **5.8.2 Unlinkability and minimal disclosure**

This issue can be tackled by using privacy attribute-based credentials (p-ABC). With this cryptographic tool, a user obtains a credential containing all of his/her attributes signed by an IdP that is trusted by the service providers. The user can then use this credential to selectively disclose specific information to the relying party, conforming to the access policy of the service. There exist working implementations that rely on p-ABCs such as Idemix, which offers minimal disclosure and unlinkability features, so the challenges are to adopt and integrate the existing p-ABC systems into applications, and to enhance their efficiency and functionality by developing novel schemes. Specifically, most of the work will be carried out leveraging the distributed p-ABC scheme developed within the OLYMPUS project [GMBS 21].

### **5.8.3 Distributed oblivious identity management**

This asset will investigate and integrate the creation of a distributed oblivious identity management system with cryptographic techniques to split up the role of the online IdP over multiple authorities. The system architecture and the cryptographic tools needed to perform said role distribution will be the baseline of the challenge.

### **5.8.4 Privacy preservation in blockchain**

This asset will investigate, integrate and adapt privacy-preserving solutions, leveraging the research being done at WP3 into self-sovereign-PPIdM (privacy-preserving IdM in blockchain), with technologies like anonymous credentials systems (e.g. Idemix) and blockchain implementations (e.g. Hyperledger). More concretely, the challenge objective is to evaluate the suitability and the application of NI-ZKP in blockchain scenarios, and to potentially develop novel NI-ZKPs with higher efficiency, smaller proof sizes, and more realistic assumptions, e.g. regarding the generation of joint parameters, etc. To this end, it is envisaged to use the outcomes from the DIF as a baseline.

### **5.8.5 Password-less authentication**

The password-less authentication asset will investigate and integrate alternative authentication methods (e.g. biometrics) that will be device-centric. The asset's architecture will be based on the FIDO Universal Authentication Framework (UAF)<sup>254</sup> and the FIDO 2<sup>255</sup> proposed by the FIDO Alliance. The main challenge objective is to design and develop a password-less authentication system that will be integrated with a privacy-preserving identity management structure. This challenge is addressed based on the research that is being done at WP3 about password-less authentication using state-of-the-art authentication protocols, such as FIDO and OpenID Connect.

---

<sup>254</sup> <https://fidoalliance.org/specs/fido-uaf-v1.2-rd-20171128/fido-security-ref-v1.2-rd-20171128.html>

<sup>255</sup> <https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.html>

### 5.8.6 GDPR guidelines and eIDAS interoperability

These assets will investigate the two prominent European regulations regarding privacy and identity management. The first will produce a comprehensive guideline on applying GDPR privacy principles while the latter will look at eIDAS interoperability issues that are currently present between the EU member states. While they are not necessarily aimed at addressing identity management, they are an important aspect when implementing such systems. and conduct studies that determine their characteristics and how they must be applied. Also, it will comprise the examination of the privacy-preserving identity management tools (and IdM in general) to ascertain how these regulations affect them.

### 5.8.7 Identity Management Solutions for the IoT

One option to address this challenge can be addressed using so-called cloud-based or encrypted attribute-based credentials, which allows one to outsource an overwhelming part of the computations to the cloud. Alternatively, a careful domain-specific requirements elicitation will lead to tailor-made solutions for specific contexts and applications.

Table 4: Challenges identified in the Privacy-Preserving Identity Management Vertical and Tools needed to address them.

Challenge	Tools required for	Tools contemplated for Privacy-Preserving Identity Management	Tools/Methods that need to be addressed
Challenge 1	System-based credential hardening	modssl-hmac (D3.1 Section 5.2)	Making leakage passwords harder to crack
Challenge 2	Unlinkability and minimal disclosure	Mobile pABC, eABCs, ArchiStar (D3.1, Section 5.1) Issuer-hiding credentials	Attribute-based credentials privacy methods and technologies
Challenge 3	Distributed Oblivious identity management	Self-sovereign identity management, Privacy Preserving Middleware, Argus, Cryptovault, Scalable and Private Permissioned Blockchain (D3.1, Section 5.1)	Distributed systems for oblivious identity
Challenge 4	Privacy preservation in blockchain	Self-sovereign identity management (D3.1, Section 5.1),	Application of privacy methods to blockchain
Challenge 5	Password-less authentication	Password-less authentication (D3.1, Section 5.1)	Alternative authentication methods
Challenge 6	GDPR guidelines and eIDAS interoperability	Guidelines for GDPR-compliant user experience and analysis of interoperability and cross-border compliance issues (D3.1, Section 5.7).	Comprehensive guideline on applying GDPR and current eIDAS interoperability issues
Challenge 7	Identity Management	eABCs	

	Solutions for the IoT		
--	-----------------------	--	--

## 5.9 Roadmap

### 5.9.1 Short-term plan

Until the end of the project, we will focus on the following aspects of Privacy-Preserving Identity Management:

- **Unlinkability and minimal disclosure.** We will improve the p-ABC scheme with Inspection and Revocation (theoretical and at least a first working implementation). We will also further advance integration with state-of-the-art access-control mechanisms. We will further analyse whether the novel concept of issuer-hiding ABCs can also be efficiently applied in other contexts (e.g. group signatures, etc.).
- **Distributed oblivious identity management.** We plan to fulfil the final goal of deployment of a distributed oblivious identity management system that fulfils the security and privacy requirements (demonstrated in the project's pilots). We also plan to integrate the new functionalities for the whole system (e.g. inspection/revocation) emerging from the last evaluation/definition cycle.
- **Privacy preservation in blockchain.** We plan to part from our first iterations to obtain a mature, functional implementation that is integrated with other components. Finally, we plan to perform benchmarking over it, to evaluate its adequacy in terms of performance.
- **GDPR guidelines and eIDAS interoperability.** In the context of the eIDAS interoperability and cross-border compliance work, we plan to examine and provide recommendations regarding the authentication mechanisms used in a selection of eIDAS national identity providers.
- **Passwordless authentication.** We intend to integrate passwordless authentication into an IdM system (e.g. Keycloak) and apply it in several scenarios (e.g. VPN, student services, etc.) to evaluate its practicality, as well as to assess possible implementation and security challenges that may arise.
- **Identity Management Solutions for the IoT.** All developed authentication schemes will be analysed for their suitability for embedded devices, and means for partially outsourcing expensive computations, e.g. to a proxy, will be considered where possible.

### 5.9.2 Beyond the end of the project plan

#### 5.9.2.1 Security 2025

While researchers are starting to achieve mature privacy-preserving identity management systems, it is still necessary to improve the current solutions to attain advanced functionalities, such as recovery (of both providers and user identities), revocation, etc., in a practical way. For this, cryptographic mechanisms and infrastructural solutions for identity management should be explored.

The current trend for highly dynamic scenarios with many devices (mobility scenarios, smart infrastructures) calls for different approaches to trust and identity management. For instance, the zero-trust paradigm, where interactions are monitored and trust is computed dynamically, is gaining traction. In this landscape, architectures and tools that enable the complex relationship between **trust and privacy** are needed, and research in those directions (trust management, SSI, federation, etc.) will be helpful.

In this context, DLTs are emerging as a promising tool for achieving trust and supporting identity management solutions. However, current implementations have multiple drawbacks, from technical issues (e.g. high energy consumption) to privacy issues. Thus, it is interesting to research better DLT implementations that reduce their drawbacks and can be applied as pivotal elements for trust, public information sharing, etc., in conjunction with privacy-enhancing tools. In this sense, the combination of smart contracts with PETs might bring transparent, auditable, enforceable and privacy-preserving interactions.

Another topic is the application of PETs in IoT devices, which are constrained by such limitations as power, battery and memory. By 2025, the number of IoT devices is expected to exceed 40 billion, more than four times the world's population. It is necessary to enable privacy-preserving identity management for IoT devices. Thus, we should pursue mechanisms for “complex” unlinkability and minimal disclosure schemes (zero-knowledge proofs, p-ABCs) that are suitable for constrained IoT devices. Additionally, we should consider architectures/solutions for whole system integrations where complex PETs coexist with other solutions, to accommodate the different ranges of devices in terms of power (e.g. delegation for the most constrained, full capabilities for non-IoT devices involved, reduced functionality for IoT devices “in the middle”, etc.).

In the forthcoming deliverable dedicated to interoperability and cross-border compliance for the eIDAS and GDPR, we will discuss some differences in how specific sections of the two regulations are implemented in the different Member States. We hope that the coming years will bring clearer rules on how to comply with the GDPR across the EU, without encountering exceptions in Member States, and that the planned revision of eIDAS will bring some more definition and guidance on how it should be implemented and how to connect to the infrastructure across the union. This would also encourage smaller companies to spread across the EU.

### 5.9.2.2 Security 2030

The fields of security and privacy are constantly in an arms race. The results obtained during the next years will need to be adapted to emerging technologies that may jeopardise security or offer better results. Specifically, close to the horizon is the more widespread and practical use of quantum computers. Thus, even though some research has already been conducted, it will become more important to evaluate the results against quantum computing and investigate how the primitives can be modified to protect systems against quantum devices while preserving practicality.

The development of robust alternative authentication methods should follow the high standards and the fast pace of the technological advances (e.g. quantum computing). To this end, during the next years, further research should be performed into alternative authentication methods in order to prepare for the new era. Moreover, a unified common evaluation framework is necessary for authentication systems that will help developers and security researchers to assess the robustness and user-friendliness of their systems.

In order to avoid cloning of attribute-based credentials, many existing schemes consider credentials that are bound to keys stored within secure hardware tokens. However, this solution suffers from usability drawbacks if such a device gets lost [BCH+ 15], or if the rightful owner of a credential wishes to use it on multiple devices. An interesting challenge will therefore be to bind credential systems to a user's biometric features, without negatively impacting efficiency, while guaranteeing the confidentiality of highly sensitive biometric data during all phases of the authentication system.

Finally, while many advanced privacy-preserving authentication mechanisms exist, they are incompatible with legacy systems used, for example, by public administrations issuing certificates with personal data. What will thus be needed is a cryptographic meta-layer that enables citizens to translate their legacy certificates into privacy-preserving counterparts, without the need to modify existing issuers. In contrast to existing approaches where, for example, SSI nodes translate a classical credential into an SSI credential, such a layer will also need to ensure end-to-end authenticity from the issuer to the verifier in order to obtain legal validity of presentations.

### 5.9.3 Milestones

By the end of the project, the remaining research tasks of different partners are expected to reach several milestones. In the following, we list the milestones identified for the research activities carried out on the different relevant challenges from the Privacy-preserving Identity Management vertical:

- Unlinkability and minimal disclosure: Research completed on the addition of new features to the p-ABC scheme, and working prototype on revocation and inspection completed and evaluated.
- Distributed oblivious identity management: Mature implementation of the distributed and oblivious identity management system integrated and evaluated in the relevant project's pilots (task 5.3 and 5.7).
- Privacy preservation in blockchain: Implementation of the blockchain smart contracts validated and tested in pilot scenarios, such as a Smart City platform with ppIdM (with the chain being a support framework for the identity aspects and also other parts of the deployment, like registration of services and monitoring), and benchmarks obtained for its performance.
- GDPR guidelines and eIDAS interoperability: Defined a set of recommendations regarding the authentication mechanisms used in a selection of eIDAS national identity providers.
- Passwordless authentication: Passwordless authentication has been integrated into the Keycloak IdM and it has been tested in the CCTV SMART Campus demo scenario of D3.13.

## 5.10 Summary

This section focused on user privacy in identity management. As explained in sections 5.1 and 5.2, current widespread identity management solutions do not enable the privacy rights of citizens or requirements of EU regulations like GDPR. Attacks by hackers and other less obvious actors like issuers or service providers (detailed in section 5.4) may harm individuals, but it can be a problem that scales to entire nations and beyond, as described in section 5.3.3.

Section 5.5.3 introduces a brief SWOT analysis that shows the strong position of EU in regard to privacy preserving identity management and how it can lead research in this area with bases in strong regulation (GDPR) and years of funded research. On the other hand, there are possible complications coming (i) from lack of standardization in the area, (ii) from little concern for privacy from companies (because of current business models), (iii) from weak awareness from users, and, finally (iv) from existing “easy to use” solutions that do not provide privacy. We see a clear opportunity for reducing service providers' control

over users and for EU to promote and contribute to standardization in the area that enables compliance to strong privacy regulations.

The recent COVID-19 pandemic has brought to light security and privacy considerations to all citizens (see section 5.5.5). Tracking applications have been proposed by different governments in an attempt to better control the spread of the virus, which has led to extensive discussion about the technical and legal aspects of citizen identification and how this vertical can contribute to mitigate or provide solutions to this scenario improving identity management features. In addition, the application of privacy regulations impacts directly with this vertical and requires an open discussion to handle it correctly.

In previous sections, we have also analysed the impact of privacy-preserving identity management in different dimensions like democracy, the green deal and EU Cybersecurity strategies. As a summary, ensuring security and privacy in identity management has a direct impact in many key topics, like enabling robust, fair and secure democratic processes, especially in online voting scenarios, or accomplishing EU regulations like GDPR. In addition, identity management has an indirect impact in almost any online scenario, as the need to identify actors is ubiquitous. In that sense, other dimensions like European cybersecurity will be indirectly impacted by the advances in privacy-preserving identity management. For instance, the relationship of identity management with the green deal might not be directly obvious, but it is necessary to take into account the great presence that identity management solutions will have. As such, the technologies applied may have a great impact on the climate (e.g., if inefficient instantiations of ledger technologies become the norm, the environment will suffer).

To try to tackle the issues related to achieving privacy-preserving identity management, we have identified seven main challenges:

- Challenge 1: System-based credential hardening
- Challenge 2: Unlinkability and minimal disclosure
- Challenge 3: Distributed oblivious identity management
- Challenge 4: Privacy preservation in blockchain
- Challenge 5: Password-less authentication
- Challenge 6: GDPR and eIDAS impact on Identity Management
- Challenge 7: Identity Management Solutions for the IoT

Addressing these challenges is the objective for the coming years. Firstly, to improve identity management systems to accommodate more variable scenarios such as the pandemic situation by paying special attention to existing regulations in order not to leave any relevant points uncovered. In addition, it is necessary to keep an open stance towards current and upcoming technologies so that we can adopt those functionalities that are interesting to improve our proposal. In that sense, the use of blockchain in combination with credentials looks to be a promising approach in terms of privacy and democratic improvement, albeit at the cost of a higher energy impact due to the high consumption that currently weighs down blockchain technology. Finally, regulations such as GDPR and eIDAS will be differentiating factors for the application of this type of privacy-preserving identity management technologies in the EU.

## 6 Incident Reporting

### 6.1 The Big Picture

The reporting of cyber and operational security incidents detected in a financial institution, which can cover a wide range from malware or ransomware infecting a bank entity network or a phishing email received by the employees to accidental events or system misconfigurations that can affect the availability of a bank website, is one of the crucial steps in the general process of incident management and response that need to be followed by any organization. This includes first the process of gathering all the information that can be related to the security incidents so it can be added to the reports to help to analyse and understand the actual severity, impact and extension of a specific incident in the context of a particular financial entity. Then, it is necessary to identify who are the recipients of the reports. In the case of incident reporting in the financial sector, there has been a significant increase in recent times in the number of regulations and legislative frameworks that apply to this sector requiring the submission of mandatory reports at different levels (e.g. EU and national level). Currently, there are no standards defined for mandatory incident reporting and procedures and timelines defined by each Supervisory Authority are diverse and without connection between them (e.g. it is required to send a first report within 2 hours of an incident classified as significant, followed by an interim report within 10 working days of first report, and a final report within 20 working days of interim report to the European Central Bank, but to the National Competent Authority it is required to send the first report within 4 hours from detection, the interim one within 3 working days of first report and the final one within 2 weeks of business back to normal). Furthermore, depending on the type of incident detected and its severity according to the specific guidelines defined by each of these regulatory frameworks, the information that need to be reported may be different. All this implies time-consuming reporting processes for the incident management and reporting teams and can even leads to delays in the overall incident response operation for the affected financial entities and a potential faster propagation of the threats.

Different stakeholders participate in the incident reporting process in the financial sector as they were described in D5.1. On the one hand, the financial institutions who are obliged to report security incidents detected according to different regulations. On the other hand, the EU/National Supervisory Authorities, who are in charge of defining the procedures and templates that need to be followed and applied and are the receivers of the reports and responsible for enhancing cyber resilience across Europe. It is also worth noting here the importance that is being given in the overall context of incident reporting to cooperation and threat intelligence data sharing among all the different stakeholders to improve the capacity and resilience of the European cyber environment and give a more efficient and quick answer to the new cyber security threats.

### 6.2 Overview

In order to benefit from the community-building activities of the Competence Centre and the Network, an instrumental step is the gathering of data on vulnerabilities and threats through appropriate and timely sharing across the industries and entities affected by cyber and operative incidents. On the one hand, a wide range of voluntary information-sharing initiatives are already in place: for instance, on the private side the Financial Service Information Sharing and Analysis Centre (FS-ISAC) initiative and on the public institutions' side the EU CERT (Computer Emergency Response Team), along with private-public cooperative mechanisms, such as the Italian CERTFin. On the other hand, European legislators have foreseen the need for Mandatory Incident Reporting and established, in the current legal provisions (e.g.

GDPR, Network and Information Security Directive (NISD), and PSD2), the need to comply with Mandatory Incident Reporting requirements towards different Supervisory Authorities. These requirements, introduced at both EU and national level, have defined various impact assessment criteria, thresholds, timing, data sets and communication means, as established by each authority.

The mandatory reporting requirements are particularly complex in the financial market. For instance, when a cyber-incident affects a multinational Financial Group, regulators established the need for each impacted entity to eventually report to the National Competent Authority the data of the incident. Meanwhile, the Parent Company Headquarters must gather all the information in a standardized way from each legal entity, in order to assess the overall impact at Group level.

This project is creating a demonstrator of a smart incident reporting platform to address the common need for standardized and coordinated cybersecurity notification. This engine will also tackle the lack of harmonization in the EU mandatory incident reporting process, which results from the existence of several different requirements that have been established at EU and national level by each supervisory authority. This tool would pave the way towards public and private cooperation towards reaching the common goal of enhanced cyber resilience across Europe and eventually beyond the EU borders.

## 6.3 What is at stake?

### 6.3.1 What is the underlying need?

The EU framework for incident reporting, arising from the evolution of the European Union's regulatory landscape, foresees the involvement of multiple competent authorities at national and European level, often applying different procedures and templates. Financial institutions need to handle multiple and fragmented incident reporting requirements in a time-critical process, whilst managing the incident itself. Among the multiple regulatory requirements that are applicable, it is worth mentioning the PSD2<sup>256</sup> (Payment Service Directive 2), the ECB SSM<sup>257</sup> (European Central Bank Single Supervisory Mechanism) and the T2<sup>258</sup> (Target2) mandatory incident reporting requirements. There are therefore mandatory incident reporting requirements arising from the EU legislation, but also from the individual national regulatory frameworks and from other mandatory requirements established in the single member states by the national competent authorities. On top of this, to fulfil the BIS-IOSCO Guidelines<sup>259</sup> (Guidance on cyber resilience for financial market infrastructures), the financial market infrastructures are introducing their procedures to enhance the

---

<sup>256</sup> Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366>), amending Directives 2002/65/EC (<https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32002L0065>), 2009/110/EC (<https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32009L0110>) and 2013/36/EU (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32013L0036>) and Regulation (EU) No 1093/2010 (<https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32010R1093>), and repealing Directive 2007/64/EC (<https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32007L0064>)

<sup>257</sup> <https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html>

<sup>258</sup>

[https://www.ecb.europa.eu/paym/target/target2/profuse/nov\\_2018/shared/pdf/Information\\_Guide\\_fo\\_TARGET2\\_use\\_rs\\_v12.0.pdf](https://www.ecb.europa.eu/paym/target/target2/profuse/nov_2018/shared/pdf/Information_Guide_fo_TARGET2_use_rs_v12.0.pdf)

<sup>259</sup> Guidance on cyber resilience for financial market infrastructures.

<https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf>

resilience of the digital single market, setting up communication flows and incident reporting patterns to coordinate the response to the attacks and to limit the systemic effect of cybersecurity attacks.

Beyond the boundaries of the financial sector, there are multiple mandatory incident reporting frameworks introduced with mandatory requirements that are applicable across multiple economic sectors. These include e-IDAS<sup>260</sup> (electronic identification and trust services), GDPR<sup>261</sup> and NISD<sup>262</sup> (Directive on Security of Network and Information Systems see Figure 10), whose applicability is cross-sectorial, and all introduce their own requirements, with their scope, templates, and timelines.

Indeed, just considering the example of the NIS Directive, the same mandatory incident reporting process is applicable to the operator of essential services (OES) and to the digital service providers (DSPs), which implies that the incident reporting framework also applies to other industries in addition to the financial sector: energy, transport, health, drinking water supply and distribution, and digital infrastructures.

OES and DSPs have to fulfil the requirements according to the rules established under the NIS Directive as defined by the designated national competent authority in the relevant member state(s). Since most of the regulatory requirements that arise under directives might be transposed in a different way across the member states, the mandatory incident reporting process becomes even more complex for those entities that operate across multiple jurisdictions.

ENISA has acknowledged that mandatory incident reporting is geared towards enhancing the cyber-resilience of the digital single market, even though it is a multilayer matter requiring cooperation among multiple stakeholders.

---

<sup>260</sup> Regulation (EU) No 910/2014 ([https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L\\_.2014.257.01.0073.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG)) of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31999L0093>)

<sup>261</sup> Regulation (EU) 2016/679 (<https://eur-lex.europa.eu/eli/reg/2016/679/oj>) of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046>) (General Data Protection Regulation)

<sup>262</sup> Directive (EU) 2016/1148 (<https://eur-lex.europa.eu/eli/dir/2016/1148/oj>) of the European Parliament and of the Council of 6 July 2016.

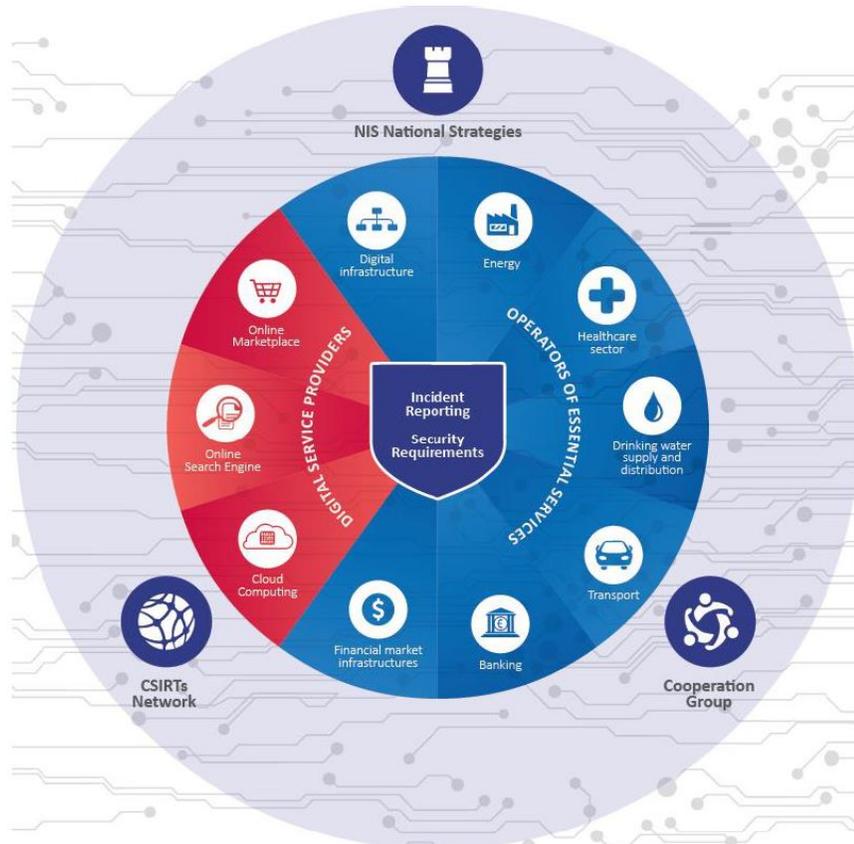


Figure 10: Graphical overview of the NIS Directive. Source: Incident notification for DSPs in the context of the NIS Directive<sup>263</sup>

All European financial institutions have to comply with the regulatory mandatory EU incident reporting requirements, but they are also involved in other voluntary initiatives at national, EU and international level (e.g. involvement in the national sectorial CERT). Moreover, banking groups have to manage further compulsory requirements arising not from legal measures, but from the involvement in different national and international financial market infrastructures (e.g. Target2), even beyond EU borders, thus entailing a huge effort that could be rationalized by creating synergies in the collection of the data necessary for the reporting of the incident.

Indeed, a single incident might entail, for a single financial institution, the need to report to multiple supervisory authorities handling the different impact assessment criteria, thresholds, timing, data set and communication means. The implementation of an incident communication smart engine would allow this regulatory fragmentation to be overcome, by streamlining the manual process of gathering the data and filling in the reporting templates according to the different requirements.

It is widely recognized that, in the absence of a common methodology and an automated process, this incident reporting activity is cumbersome and could create issues with respect to meeting the deadlines and

<sup>263</sup> Incident notification for DSPs in the context of the NIS Directive. ENISA. February 27, 2017 <https://www.enisa.europa.eu/publications/incident-notification-for-dsps-in-the-context-of-the-nis-directive>

the consistency standards of the data required in the incident reporting process. This has also been highlighted by the European Banking Federation in its position paper on cyber incident reporting.<sup>264</sup>

It is worth mentioning that in their recent joint advice<sup>265</sup>, the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA) have recognized such fragmentation and have proposed that “**existing incident reporting requirements should be streamlined (...) standardising reporting templates and timeframes where possible**”. Meanwhile, the financial institutions have to cope with this complexity in order to comply with the fragmentation of the regulatory requirements that are already in force.

### 6.3.2 What is expected to go wrong?

An effective solution for incident reporting should cover the necessary requirements to make sure that the reporting is protecting the interests of all the parties contributing information and is delivering utility and high value to them. Even though legislation and regulatory conditions impose an obligation on many of the stakeholders involved, the ultimate motivation for adoption and compliant delivery of incident reports will come from (a) the experience of *benefits (value) in contributing*, and (b) the *absence of enhanced risks and additional damage* for the contributors.

The strength of an incident reporting utility demands many insights and many contributing disciplines. The research roadmap probably demands an iterative improvement and refinement of capabilities that allow an incident reporting system to dynamically grow and evolve, thus showing and illustrating the feasibility of intermediate versions – with growing subsets of the envisaged functionality.

The perceived *value* of an incident reporting system includes the following aspects:

1. The capability of dealing with a broad variety of types of incident, and varying degrees of sophistication in information provisioning. The former is an obvious inroad to encourage the prompt reporting of all incidents; the latter offers the ability to contribute while being only partially aware and/or informed about essential parts of the information that completely describes an actual incident.
2. The capability of prompting the reporting party with questions and suggestions on how to complete the information, and how to relate and classify incidents in the right clusters and families.
3. The capability of associating incidents with known vulnerabilities that enable attackers and campaigns to cause damage to services, users and organizations. At the same time, the link to specific known vulnerabilities will obviously enable preventive remediation.

<sup>264</sup> EBF position on cyber incident reporting:

<https://www.ebf.eu/wp-content/uploads/2019/10/EBF-position-paper-on-cyber-incident-reporting.pdf>

<sup>265</sup> *Joint Advice of the European Supervisory Authorities: to the EC on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector – 10 April 2019.*  
<https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/4d2ad5e2-1570-48bd-819a-7cd9b4e8b157/JC%202019%2026%20%28Joint%20ESAs%20Advice%20on%20ICT%20legislative%20improvements%29.pdf?retry=1>

4. Automatic access to related incidents, vulnerabilities and countermeasures should be the obvious reward for the contributing stakeholder.

The *absence of additional damage* is an essential additional criterion that must be addressed in order to be successful. Reporting an incident can cause reputational and business damage if the information is by default available to all stakeholders and without restrictions on the amount and level of details that are made available to observers.

1. Incident reporting can be of lower risk and relatively more acceptable if the provided information is largely *anonymized* with respect to the party that reports damage while being a victim of a cybersecurity incident.
2. In addition, *access control* to the provided information must be strong, to guarantee that users of the information are restricted to the parties that have the formal rights to access the information, and that have undertaken to treat this information in line with the terms and conditions imposed by an incident reporting platform/utility.
3. *Usage control* of the information being accessed by the stakeholders obviously is of equal importance.
4. As existing techniques for access and usage control are inherently limited, there is an obvious need for *audit trails* that enable the inspection and analysis of external and internal users of the incident reporting platform.

Both categories of requirement stress the value of the available information and the trustworthiness of the platform. They will both contribute to the acceptance of an incident reporting utility. If these matters are not addressed, low utilization and limited acceptance would be the consequence.

Additional needs emerge if the basic successes are achieved. Given the feasibility, value and trustworthiness of the incident reporting utility, many stakeholders may pick up the capability and effectively use it. This can ultimately lead to a scenario of high utilization.

The effectiveness of the system in case of high utilization depends on a set of “standard” requirements that will become more and more relevant as the scale of the deployment further increases.

1. The quantity of incidents that are being reported, analysed and covered will increase, automated vetting and classification will be an essential element to enable scalability.
2. Similarly, the versatility of the type of incidents and associated contextual information requires heterogeneity, automated harmonization, etc.

The intelligence of the incident reporting utility as sketched above is one important element, alongside other, rather standard requirements that come with large-scale deployment. These include

1. Performance of large-scale deployments
2. Availability and resilience of the utility/service, especially in times of peak loads and crises.

A last essential dimension of success includes the overall use-ability that comes with a number of facets: (1) the immediate quality of the front-end dashboard that is made available for different types of stakeholders; (2) the quality of the automated reporting; and (3) the capabilities of operators and analysts to deal with large scale incidents and campaigns.

The summary sketched above lists a broad range of needs and demands for the incident reporting systems. Each of these defines a threat in its own right when not being addressed. Yet the most important threat of not delivering on the potential comes when stakeholders cannot trust the platform to protect sensitive information, thus causing additional damage because of reputational damage or business damage.

### 6.3.3 What is the worst thing that can happen?

If an organization does not report a cybersecurity incident, then the accident remains unknown to the public; this prevents other organizations from implementing preventive countermeasures against such an incident. This situation, if repeated, will lead to complete freedom for attackers: once successful, the attackers will repeat the same attack against various organizations, with a good chance that the repeated attacks will also be successful.

As a result, the worst types of impact provided by Joint Research Centre, a European Commission science and knowledge centre [JRC 2019], and identified in the case incidents are not reported are the following

- **Harm to Operations:**
  - *Inability to perform current missions/business functions:* without proper knowledge of ongoing cyber incidents, an organization will not have a proper defence from modern attacks, and therefore, is likely to suffer from serious losses if attacked.
  - *Inability, or limited ability, to perform missions/business functions in the future:* in case of several successful attacks, an organization is likely to lose the trust of customers and go bankrupt.
  - *Harms (e.g. financial costs, sanctions) due to noncompliance:* complex regulations cannot be implemented.
  - *Relational harms:* Trust relationships between organizations are lost, because the organizations cannot be sure if their partners are reliable and can guarantee the integrity and confidentiality of exchanged information.
- **Harm to Assets:**
  - *Damage to or loss of physical facilities:* terrorist attacks take advantage of untrusted relations between the organizations to damage physical facilities, also causing human casualties.
  - *Damage to or loss of information systems or networks:* traditional cyber-attacks, such as ransomware, relentlessly disable the underlying IT infrastructure as its defence system is not prepared for the modern attacks.
  - *Damage to or loss of information assets:* Various information assets are tampered with by malicious adversaries, rendering the knowhow and intellectual property of companies useless.
  - *Loss of intellectual property:* IP gets routinely stolen from corporations and governments which are not even aware of the incidents.
- **Harm to Individuals:**
  - *Injury or loss of life:* counterfeited or tampered products affect people either directly or indirectly.
  - *Physical or psychological mistreatment:* the public cannot trust the safety of the products they use in their daily lives.

- Harm to other organizations:
  - *Relational harms*: The absence of incident reporting damages relations between all the actors involved if the ecosystem can no longer be trusted.
- Harm to the Nation
  - *Relational harms*: loss of trust relationships with other nations, loss of national reputation, loss of national security due to the inappropriate defence conditions of the critical infrastructure.

## 6.4 Who are the main stakeholders?

Aiming at improvement of the cyber-resilience of the digital single market, the EU mandatory incident reporting framework establishes mandatory reporting requirements for financial institutions and for several other economic sectors. Therefore, the main stakeholders of a common methodology and an automated process for incident reporting within this context are:

- **Financial Institutions**: financial institutions are subject to many regulations and frameworks that require mandatory incident reporting to several supervisory authorities and/or international financial market infrastructures, according to specific procedures and by means of different templates. Within the financial market, mandatory incident reporting requirements apply to:
  - **Target 2 Critical Participants** (ECB Target2): Participants in the Target2 payment system are classified as critical participants or as non-critical participants, depending on their market share in terms of value and/or on the type of transactions they process.
  - **Significant Institutions** (ECB SSM): The ECB classifies banks as significant or not significant based on the following criteria: size, economic importance, cross-border activities and direct public financial assistance.
  - **Payment Service Providers** (PSD2): Financial institutions operating as payment service providers (PSPs).
  - **Operators of Essential Services** (NIS): Financial institutions can be considered as OES if they fulfil the following criteria: (a) they provide a service that is essential for the maintenance of critical societal and/or economic activities; (b) the provision of that service depends on network and information systems; and (c) an incident would have significant disruptive effects on the provision of that service.
  - **Personal Data Processors/Controllers** (GDPR): Financial institutions can operate both as processors, which process personal data on behalf of a controller, and as controllers, which determine the purposes and means of the processing of personal data.
  - **Trust Service Providers** (eIDAS): Financial institutions can operate as either a qualified or a non-qualified trust service provider.
- **Regulators**: European or national legislative entities responsible for proposing and adopting the laws that regulate the functioning of specific areas of activity. At the European level, the main regulators are the European Commission, the European Parliament, and the Council of the European Union, as well as, for the financial sector, the ECB. At the national level, the main regulators are

national Parliaments. For the financial sector, national Central Banks and Securities Commissions (e.g. the Italian Consob) are entitled to define rules and guidelines applicable to national financial institutions.

- **EU/National Supervisory Authorities:** Entities responsible for the direct supervision under EU normative or national transposition laws and regulations. The responsible authorities are defined at EU or at national level and will be the recipients of the corresponding mandatory incident reports. Each regulation defines one or more corresponding authorities and additional mandatory incident reporting requirements, such as the obligation to notify a national authority in addition to the EU authority specified in the EU normative, can be defined and applicable at national level:

- **NIS Directive:** National NIS Authority
- **GDPR:** National Data Protection Authority
- **eIDAS Regulation:** National Certification Authority
- **PSD2:** NCA/ECB/EBA
- **ECB/SSM:** ECB/Joint Supervisory Team
- **Target2:** National Central Bank/ TARGET2

- **International Financial Market Infrastructures**

- **Target2:** The payment system owned and operated by the Eurosystem establishes Mandatory Incident Report requirements for those of its participants that are classified as Critical Participants, according to the following criteria: market share in terms of value and/or the type of transactions processed.

Some of the qualifications that apply to Financial Institutions, e.g. OES or Personal Data Processors/Controllers, can also be applied to other entities from other business or public sectors that could be involved in the use of the demonstrator as stakeholders in a later phase. These are:

- **Operators of Essential Services (NIS):** Entities belonging to various economic sectors considered as OES by the respective national government, taking into account the following criteria:
  - a) the provision of a service which is essential for the maintenance of critical societal and/or economic activities;
  - b) the provision of that service depends on network and information systems;
  - c) an incident would have significant disruptive effects on the provision of that service.
- **Personal Data Processors/Controllers (GDPR):** The Data Controller is the natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data. The Data Processor is a natural or legal person, public authority, agency or other body that processes (e.g. collects, records, organizes, stores, uses, etc.)

personal data on behalf of the Controller. In case of a personal data breach, the duty of notification to the Supervisory Authority belongs to the Controller, which, in turn, must be first notified by the Processor without undue delay.

- **Trust Service Providers (eIDAS):** Trust service providers are classified as qualified or non-qualified.

In a wider perspective, other stakeholders that might benefit from an automated process of incident reporting and an enhanced cooperative approach to information sharing are:

- **European Union agencies**

- **ENISA:** ENISA supports Member States and European Union stakeholders in their response to large-scale cyber incidents that take place across borders, in cases where two or more EU Member States have been affected. Moreover, it also supports the development and implementation of the European Union's policy and law on matters relating to network and information security (NIS) and assists Member States and European Union institutions, bodies and agencies in establishing and implementing vulnerability disclosure policies on a voluntary basis.

- **Law-enforcement agencies**

- **Europol:** in particular, through the European Cybercrime Centre (EC3), strengthens the law enforcement response to cybercrime in the EU and helps to protect European citizens, businesses and governments from online crime also by leveraging the information voluntarily shared by the private sector.

- **European citizens:** in a wider long-term perspective, the final beneficiaries of the deployment of smart incident reporting tools are the European citizens. They will indirectly benefit from an enhanced resilience and security in the Digital Single Market, resulting from the increased information sharing on cyber vulnerabilities and threats.

## 6.5 Major incidents in this vertical

Over the past years, several incidents and cyber-attacks have occurred around the world, and many of them prompted the financial institution to strengthen its defences. Cyber-attacks targeting financial institutions are becoming more frequent, sophisticated, and destructive. The main threat is cyber-attacks followed by data breaches. The following are some of the most relevant events that occurred worldwide.

- Cyberattack on Bangladeshi bank (April 2016). Cybercriminals stole \$81 million from a Bangladeshi bank through the use of malicious code. This malware allowed the attackers to access the messaging software known as SWIFT Alliance Access. A year later, Russia's central bank suffered a similar attack in which the attacker stole \$6 million.
- Malware targeting Polish banks and institutions in Latin America (February 2017). Several Polish banks and some Latin American banks were victims of a watering hole attack, which, thanks to a trusted site that was compromised, redirected to a fraudulent page hiding an exploit. In the case of Polish banks, the starting point was the website of the Polish Financial Supervision Authority.

- WannaCry Ransomware (May 2017). On 12 May, 2017, the WannaCryptor infected thousands of computers across the world. After just 24 hours, the number of infections had spiked to 185,000 machines in more than 100 countries. It can spread within the network by exploiting a particular network communication protocol weakness that enable attackers to install the ransomware remotely on to OS windows-connected hosts.<sup>266</sup>
- Equifax data breach (October 2017). In one of the biggest data breaches on record, the credit reporting agency Equifax announced in October 2017 that more than 150 million customer records had been compromised, including some sensitive data such as birth dates and 12,000 U.S. social security numbers. According to the U.S. government indictments, the breach was carried out by the Chinese People’s Liberation Army (PLA) and exploited a bug in an Apache Struts web application that the company had failed to patch.<sup>267</sup>
- Cyberattack affects Mexico’s financial system (May 2018). Mexico’s financial system was the victim of a cyber-attack in which criminals stole close to 300 million Mexican pesos (€12,400,401). The incident began in the system of interbank electronic payments (SPEI), which began to report failures, and later proceeded to exploit a vulnerability in the web service that connected the systems with SPEI. The attackers were able to make unauthorised transfers.
- Cosmos Bank SWIFT Heist (August 2018). In August 2018, it was reported that Cosmos Bank, the second-biggest cooperative bank in India, lost \$13.5 million through ATMs in 28 countries, as well as through unauthorised interbank transactions. The attack left Cosmos’s online banking service offline for more than a week, and the funds have not been recovered. There were signs that an attack on a bank was coming. Two days before the incident, the FBI issued a warning to banks about an imminent ATM cash-out scheme, without providing further public details. In August 2019, the UNSC Panel of Experts indicated DPRK-affiliated actors were behind the attack.<sup>268</sup>
- Cyberattack on the European Central Bank (May 2019). The European Central Bank announced that one of its websites was attacked by unauthorised persons, causing a leak of confidential information. The attackers installed malware on an external server hosting the BIRD data management system to facilitate phishing activities. The impact was a leakage of sensitive information in 481 BIRD newsletters.
- Hong Kong Exchanges and Clearing Limited DDoS Attack (September 2019). On September 6, 2019, Hong Kong Exchanges and Clearing Limited (HKEx), a Hong Kong-based stock exchange, suffered a distributed denial-of-service attack (DDoS) and discovered a technical bug, forcing them to suspend trading.<sup>269</sup>
- SolarWinds (2020) Earlier in 2020, hackers broke into SolarWinds’ “Orion” system, an IT-management instrument used by multiple U.S. government agencies and many major companies. The hack appeared to be the work of state-sponsored actors operating out of Russia. Although no initial reports indicated that major U.S. banks were targets, FS-ISAC has been partnering with Wall Street to offer strategic risk mitigation strategies.<sup>270</sup>

---

<sup>266</sup> Source: Kaspersky Lab Report

<sup>267</sup> Source: <https://carnegieendowment.org>

<sup>268</sup> Source: <https://carnegieendowment.org>

<sup>269</sup> Source: <https://carnegieendowment.org>

<sup>270</sup> Source: <https://carnegieendowment.org>

- Destructive cyberattack hits National Bank of Pakistan (October 2021) The National Bank of Pakistan suffered a cyber-attack that took down part of its infrastructure. The attack impacted the bank’s backend systems and affected the servers used to interconnect the bank’s branches. The attacker gained access to a privileged Active Directory account and used it to deploy malware on the systems. As a result, the bank’s ATM network and mobile apps became unavailable.
- Cyber Attack shuts down Ecuador’s largest bank, Banco Pichincha (October 2021). The Ecuadorian bank, Banco Pichincha, suffered a cyber-attack that interrupted operations and put the ATM and the online portal out of service. Different sources affirm that it was a ransomware attack, in which the threat actors installed a Cobalt Strike beacon in the bank’s network. The impact was unavailability of services.

## 6.6 Research Challenges

We have identified three main research challenges and issues that we will try to investigate and address within and beyond the current project regarding the underlying needs identified for incident reporting:

Previous sections have analysed how different dimensions (such as green and climate dimensions, COVID-19 and sector-specific dimensions) impact on incident reporting in the financial sector and/or how this vertical can contribute in some way to those dimensions. As a summary, given the indirect impact it can have on different dimensions for citizens, the importance of fighting and preventing cyber-attacks against financial institutions can be highlighted, not only for its economic impact, but also to increase the reliability and trustworthiness of users in these institutions. This links directly with the need to improve the methodologies and tools used in this vertical for efficient and rapid information gathering, and reporting information about the cyber-incidents detected to the competent authorities. To foster collaboration by sharing threat intelligence data between stakeholders in the financial sector is also a related key point. On the other hand, another recurrent topic in the analysis is the disparity and number of different existing regulations that require mandatory incident reporting, as that applies to the financial sector. This has a negative impact in the vertical because this fragmentation and lack of unification in the requirements implies complexity, which translates into an increase in the costs and time spent on incident management. Consequently, the results of the analysis of these dimensions have helped us to better identify which challenges and developments we need to include in the roadmap.

- Challenge 1: Lack of harmonization of procedures
- Challenge 2: Facilitate the collection and reporting of incident and/or data leaks
- Challenge 3: Promote a collaborative approach for sharing incident reports to increase risk quantification, mitigation and thus overall cyber resilience

The challenges for this case are indexed to their corresponding JRC taxonomy sectors and presented along with a description for this vertical.

### 6.6.1 State of the Art

The previous version of the “Research and Development Roadmap” [Markatos 2020] included an overview of the stakeholders at stake involved in the process of incident reporting in the financial sector with their needs, the regulatory background affecting this sector, the potential impact in case the incident was not reported and it was identified the main research challenges related. This section provides a state of the art focused on security incident reporting although we have also included a short overview on risk assessment methodologies that could be applied on incident reports. The description of the state of art related to cyber

threat intelligence data sharing, which is also a research challenge for this vertical, can be found in the deliverable D3.3 Research challenges and requirements to manage digital evidence [PJB+ 2020].

### 6.6.1.1 Security incident reporting

Although reporting is one of the key steps always present whenever a security incident takes place, there is not an agreement or a common procedure to be followed for incident reporting, even in a same sector such as the financial one.

We can find many guidelines and procedures on incident reporting, published by different entities, to help organisations and security managers to be compliant with a specific regulation or to tackle incident management in general. For example, the ISO/IEC 27035 standard on “Information technology – Security techniques – Information security incident management” [ISO/IEC 27035] provides guidelines related to this topic. ENISA<sup>271</sup> provides support to the EU telecom security authorities for telecom security breach reporting, with a technical guide on incident reporting to cope with Article 13a of the EU Directive 2009/140/EC related to electronic communications<sup>272</sup>; to Supervisory bodies for EU trust services security breach reporting under the eIDAS regulation with a proposal for an incident reporting framework<sup>273</sup>; and to the Commission and the EU member states with a report containing guidelines on reporting NIS Directive breaches.<sup>274</sup> ENISA also offers a visual tool named “CIRAS”<sup>275</sup> (Cybersecurity Incident Report and Analysis System), which publishes anonymised and aggregated data from security incidents with significant impact reported by the EU telecom operators and trust service providers.

Other institutions also provide different reports with lists of recommendations, steps or phases to be followed throughout the incident response lifecycle, and references to consult, such as the latest NIST guidance on tackling ransomware attacks published on September 2021 [NISTIR 8374] by the National Institute of Standards and Technology (NIST), or the CREST Cyber Security Incident Response Guide.<sup>276</sup>

The literature also includes more specific documents for reporting to different national supervisory authorities. Some examples are the recently revised Guidelines on major incident reporting under PSD2 published by the European Banking Authority,<sup>277</sup> the document “Cyber Incident Reporting – A Unified Message for Reporting to the Federal Government”<sup>278</sup>, provided by the US Department of Homeland

---

<sup>271</sup> <https://www.enisa.europa.eu/topics/incident-reporting>

<sup>272</sup> Technical Guideline on Incident Reporting. Technical guidance on the incident reporting in Article 13 a (Version 2.1, October 2014) ENISA.

<sup>273</sup> Proposal for Article 19 Incident Reporting. Proposal for an Incident reporting framework for eIDAS Article 19. Dr. Konstantinos Moulinos, Dr. Marnix Dekker, Christoffer Karsbert. December 03, 2015. ENISA.

<sup>274</sup> Incident notification for DSPs in the context of the NIS Directive. February 27, 2017. ENISA.

<sup>275</sup> <https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool>

<sup>276</sup> Cyber Security Incident Response Guide. Jason Creasey and Ian Glover. 2013. <https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf>

<sup>277</sup> <https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2>

<sup>278</sup> <https://www.dhs.gov/publication/cyber-incident-reporting-unified-message-reporting-federal-government>

Security, or the Australian Government Information Security Manual,<sup>279</sup> with information about when it is necessary to report a cyber-security incident, which information to include and the points of contact for making the report.

The growing quantity of existing regulations and legislation addressing cyber security incidents has created a need for studies on cybersecurity incident reporting for specific areas. In particular, for the financial sector we can find a report published by the Financial Stability Board (FSB),<sup>280</sup> with an analysis on existing approaches for cyber incident reporting, or the list of reporting resources included in the Cybersecurity Resource Guide for Financial Institutions, published by the United States interagency body Federal Financial Institutions Examination Council (FFIEC).

However, if we search for available tools to help in this relevant task, we will find there is a lack of solutions focused on the management and generation of mandatory incident reporting according to different regulatory frameworks, even though the feature “report incidents” is included in many of them. Indeed, most SIEM (Security Information and Event Management) solutions available on the market, such as IBM QRadar<sup>281</sup>, Alienvault USM<sup>282</sup> or Splunk<sup>283</sup> (just to name a few), provide a means of generating reports about the security incidents detected. However, these reports do not follow any common template and the information included in them does not cover what is required for mandatory incident reporting to the different Supervisory Authorities.

If we focus on open source tools available specifically for incident reporting, in the context of incident management and response we can highlight the following: Cyphon<sup>284</sup>, TheHive<sup>285</sup>, Fast Incident Response Platform (FIR)<sup>286</sup>, GRR Rapid Response<sup>287</sup> or Mozilla InvestiGator (MIG)<sup>288</sup>. The main advantages of Cyphon are that it is integrated with the ELK stack (Elasticsearch, Logstash and Kibana) and it is possible to customize the incoming data model. However, the user interface (called Cyclops) has a non-commercial use license, it is not integrated with the open source threat intelligence platform MISP and it does not include any ticketing system, which could be necessary to implement an incident reporting workflow. FIR offers a simple, extensible and customizable tool written in Python, but the main disadvantage of this tool is that it includes only basic incident response functionalities and it is not integrated with MISP. GRR includes among its advantages that it is scalable and supports automated scheduling for recurring tasks, but it is more focused on remote live forensics than on reporting. The Mozilla InvestiGator tool is easy to deploy and use and uses AMQP (Advanced Message Queuing Protocol) to distribute actions, but it is currently deprecated and no longer maintained by Mozilla. TheHive seems to be one of the best open source solutions in the

---

<sup>279</sup> Australian Government Information Security Manual. Australian Cyber Security Centre. March 2019.

[https://www.cyber.gov.au/sites/default/files/2019-03/Australian\\_Government\\_Information\\_Security\\_Manual.pdf](https://www.cyber.gov.au/sites/default/files/2019-03/Australian_Government_Information_Security_Manual.pdf)

<sup>280</sup> <https://www.fsb.org/>

<sup>281</sup> <https://www.ibm.com/es-es/products/qradar-siem>

<sup>282</sup> <https://cybersecurity.att.com/products>

<sup>283</sup> [https://www.splunk.com/en\\_us/software/enterprise-security.html](https://www.splunk.com/en_us/software/enterprise-security.html)

<sup>284</sup> <https://www.cyphon.io/>

<sup>285</sup> <https://thehive-project.org/>

<sup>286</sup> <https://sectechno.com/fir-fast-incident-response-platform/>

<sup>287</sup> <https://github.com/google/grr>

<sup>288</sup> <http://mozilla.github.io/mig/>

market for various reasons: it provides integration with MISP and, through Cortex<sup>289</sup>, with a huge number of available analysers. Furthermore, new analysers and responders can be easily implemented and integrated. It also supports the creation of new incidents through templates defined by the user or directly from emails or alerts generated by other tools (such as SIEMs), and it includes the ability to define tasks and assign them to users. Additionally, TheHive is an active project with a supporting community to solve bugs and implement enhancements. The main disadvantages of this tool are its limited case template customization and the fact that it supports only limited workflow enforcement—for example, it has no role management associated with the incidents. The new version, TheHive4, attempts to solve some of these constraints, including for example RBAC (role-based access control) features, but there are still many limitations and it is not yet a stable version.

Other open source tools related to incident reporting, but in this case more focused on the incident management, are the issue tracking systems or ticketing systems. Some relevant examples are: Request Tracker for Incident Response (RTIR)<sup>290</sup>, osTicket<sup>291</sup> and Open Technology Real Services<sup>292</sup>. In particular, RTIR is interesting because it provides preconfigured workflows designed for incident response, support custom roles management and a flexible email templating system. However, it does not offer MISP integration and its features are more related to a ticketing system than to incident management and response. Finally, we can also mention some interesting open source reporting tools for pentesting, such as Dradis<sup>293</sup>, MagicTree<sup>294</sup> and Metagoofil<sup>295</sup>. They offer the possibility of generating reports but focused on the testing performed.

### 6.6.1.2 Risk assessment methodologies on incident reports

Sources of information about breaches and advanced threats are fragmented and are mainly produced by industries rather than academic publications. As a result, the lack of standards generates unstructured reports that cannot be analysed easily. Key-search automated approaches for data extraction cannot be applied because they produce a high number of false associations in the reports analysed.

This unstructured data makes the analysis of risk challenging and thus forces the application of qualitative risk assessment methodologies. For example, NIST proposes the use of a “risk matrix”, where the likelihood of a threat event is classified as low, moderate, or high [NISTIR 2021]. Similarly, the International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC) has the ISO27K information security standards for assessing the risk of an information management system. The effectiveness of these approaches in deciding on proper responses has been questioned. A common procedure would then make it possible to define quantitative risk assessment methodologies that make automated use of the data from these incidents. The goal would be to objectively estimate the likelihood of attacks against an infrastructure, leveraging the large amount of data available from the IT infrastructure.

---

<sup>289</sup> <https://github.com/TheHive-Project/Cortex>

<sup>290</sup> <https://bestpractical.com/rtir>

<sup>291</sup> <https://osticket.com>

<sup>292</sup> <https://otrs.com/>

<sup>293</sup> <https://dradisframework.com/ce/>

<sup>294</sup> <https://www.gremwell.com/>

<sup>295</sup> <http://www.edge-security.com/metagoofil.php>

This would make it possible to experimentally evaluate the efficacy of an attacker's campaigns and the efficiency of different mitigations by means of realistic models obtained from the incidents reported.

To increase the reliability of the qualitative methods, the more structured approaches based on the qualitative system assessment has been proposed. For example, CORAS [LSS 2010] actively uses the graphical models to support the analysis steps and validate the results, while SREP [MFMP 2006] integrates the security related requirements into the software development process on the early stages of a development process. The further comparison of the visual-based versus text-based risk-analysis approaches [LMP+13] suggested that the visual method is more effective in threat identification as the threat diagrams help brainstorming the threats. On the other hand, the textual method provides better results when identifying security requirements because the process helps identification of the requirements with higher quality.

A possible future improvement of the risk assessment methodologies lies in the application of the application of the automated anomaly detection techniques. Similar approach has been proposed within the FLYSEC and the TRESSPASS EU funded projects in the context of security-based checking of travellers [Thomopoulos 2021]. In this respect, deep learning and artificial intelligence techniques provide promising results, as they are capable of automatically identifying subtle features of the analysed system. Hence, compared to the expert-based qualitative risk assessment methodologies, the deep learning-based risk assessment systems have the potential to reduce bias in estimating the security risk of an analysed information system.

## 6.6.2 SWOT Analysis



Figure 11: Incident Reporting SWOT Summary

The creation and deployment of a powerful, international and versatile incident reporting platform is without any doubt a challenge involving many facets. These range from the purely technical aspects of functional and non-functional requirements, over the essential security aspects of the platform itself, to the organizational, process-related and procedural facets that guide and drive the successful deployment of such an international incident reporting platform.

This subsection summarizes our major findings in a SWOT analysis (see Figure 11) when considering a European endeavour to develop and deliver the envisaged result.

### 6.6.2.1 Strengths

This subsection summarizes our major findings in a SWOT analysis when considering a European endeavour to develop and deliver the envisaged result.

The EU has established a long-standing tradition of collaboration amongst the various stakeholders, and a willingness and culture to make such a complex collaboration and orchestrations happen. This never comes

easily. Multilateral agreements and joint efforts must converge in an inherently heterogeneous context; this remains nontrivial. Yet there is a specific strength that comes into play and may bring an edge to a European initiative. We summarize the highlights.

We stress that incident reporting has long-term value for all stakeholders and contributors in that it can increase our common strength in threat intelligence.

- There is a **European awareness and a quest for the essential added value** that should come with reporting. Recent investigations, particularly academic research in the area of threat intelligence (TI) have shown that there are significant shortcomings in the “default” commercial approach towards TI – TU Delft, amongst others, has been playing a strong and leading role in this respect.
- There is consequently a **common understanding that open competition will not pay off or will be insufficient** in this respect. An analysis of TI practices clearly illustrates that there is insufficient value in stove-piped parties gathering fragmented information and translating this into priorities for a (too) narrow user base.
- **The community mind-set and collaborative nature** of a truly successful incident reporting initiative appears to be a European asset, from the perspective of the culture of collaboration. Indeed, there is a strong collaborative attitude and trust among stakeholders who are willing to agree upon, design and implement relevant reporting workflows and bridge the gap in terms of process and organisational barriers.
- **The EU could hit the ground running.** Most requirements related to cyber incident reporting have been articulated and established by different supervisory and regulatory authorities. This has been manifested at national levels, at the European level and within industry segments. These reporting requirements have to be harmonized and streamlined. Yet they represent a comprehensive baseline to build upon and to ensure that all relevant information about the cyber security incident or data leak is reported.
- **The EU has the talent pool to cover all bases.** The delivery of a pragmatic and incrementally growing solution demands many disciplines and operational experience. The EU has the people and the leadership to make this happen. This requires expertise in a mix of domains that consider purely technical aspects of functional and non-functional requirements of a platform, over essential security aspects of the platform and the way it is deployed, to organizational needs and approaches, as well as process-related elements, procedural facets and a deep understanding on meeting regulatory requirements and achieving compliance.

#### 6.6.2.2 Weaknesses

The effective realization of an incident reporting platform is a long-standing project that confronts us with some limitations. Some of these are grounded in our weaknesses.

- **Cost:** This platform cannot be delivered with small budgets. It seems feasible and effective to maximize the utilization of open source software in the overall architecture and solution; yet this is not a free lunch either. The development, testing, architecture and support remain significant – so is the value afterwards.
- **The high risk of dealing with the inherent complexity of this subject matter is substantial.** Regulatory fragmentation and duplication make it difficult to have one single interpretation/translation of obligations and compliance requirements into technical mechanisms. Therefore, the

time needed to roll out qualitative and stable, well agreed upon platforms and practices, remains significant.

- **The operational overhead (in terms of human resources)** of managing the additional responsibilities. Regulatory fragmentation, establishing different taxonomies, thresholds, timing, templates and information requirements to report a cybersecurity incident and/or data leak **increases complexity and administrative burdens** for all organizations and companies involved. In the current context, where human capital is stretched by a lack of talented human resources for cybersecurity, it will be hard to dedicate and divert such resources from where they are also urgently needed, especially when a cybersecurity incident occurs. It goes without saying that reliable automation is a necessity; this in fact is an opportunity, but also a substantial challenge, and we will still need humans in the loop.
- **Technology is not available off the shelf**, even though many building blocks are available: both in the public domain (open sourced) and through commercial vendors. Building the platform from scratch is not a realistic option, an architecture that assists in taking decisions whether to make or buy will be instrumental to success.
- An end-to-end solution that (probably) combines a central authority with a federated approach that leaves part of the data and details in countries and enterprises, demands a distributed infrastructure that inherently exposes a significant **attack surface** that must be hardened, protected and monitored in its own right. This challenge might be unprecedented and it is therefore fair to state that the EU as a community may reach its limits in terms of skills, people and practices to ensure a stable rollout. Is this a weakness? Not entirely. It is more of an awareness of the inherent challenges ahead.

### 6.6.2.3 Opportunities

The gradual creation, implementation and validation of an incident reporting platform is extremely challenging, and despite the challenges that may also stress our weaknesses, quite a lot of exciting opportunities unfold when we look into the future. Here is an overview of the most important opportunities.

- Given the legislation and regulatory obligations that are imposed on companies, it is clear that one significant opportunity is in the **reduction of the effort**, and of the complexity and administrative burden companies have to face when reporting a cybersecurity incident and/or data leak. In fact, this burden would be hard to take on, if not unfeasible, without a generally available platform for incident reporting. This is the first and most obvious opportunity ahead.
- In addition, and assuming a successful multilateral collaboration, the incident management **process** for various organizations will be **improved**. This is inherently possible when a lot of the information stored in the incident reporting platform can also be analysed by individual organizations to detect/observe trends and to determine the mitigation measures that have to be adopted after an incident has occurred.
- Incident reporting is not a standalone goal. The **contributor will benefit** in the short and long term from reporting and therefore being compliant with future legislation. For organisations with high stakes in terms of possible risks, business continuity when facing substantial breaches, etc., incident reporting is a small piece of the complex risk and cybersecurity management puzzle. In fact, we expect that the **incident reporting capabilities will be integrated** – at the level of individual organisations, as well as at the level of supporting bodies, governmental or private service providers

- **into fully-fledged environments for incident management.** In other words, the front end of an incident reporting platform can be leveraged in an end-to-end incident management environment.
- Such an integrated incident reporting platform can obviously – in principle – support many types of players. We can foresee that a more generically powerful capability can be extended with **specialization for specific segments**, not only towards industries but also to other types of special interest groups: ranging from individual citizens to sector federations in finance, healthcare insurance etc.
- The midterm return value from an integrated reporting platform is its potential intelligence. **Enhanced threat intelligence will subsequently flow back to the contributors**, backing many stakeholders in the process of organizing preventive defence and staying sufficiently ahead of the game. In other words, submitting information about previous incidents should and will yield a return in terms of advice, knowledge and tangible support in incident handling and incident prevention.
- Finally, it is worthwhile to stress the need for strong and appropriate real-world access control in the deployment and utilization of this incident reporting system. This remains a non-trivial need in practice, and it may and should help – as a killer application – in **collectively moving forward in the space of real-world access control and usage control**. In addition, solid audit trails must be developed and supported; this brings another reference case for the adoption of advanced security technologies in industry and society.

#### 6.6.2.4 Threats

There are several threats for this vertical as explained below:

- **A project hard to manage.** Due to the presence and involvement of many stakeholders, the decision making, and project planning and delivery may be inherently cumbersome and risky.
- Because of its **inherent complexity**, the project would demand a gradual approach, implementing intermediate and partial versions that can initially be validated and deployed by subgroups (of the broad and versatile target audience). Yet such a gradual implementation may create a **perception** of a minimalistic delivery in the early stages. This definitely has to be combined with strong communication, especially when the results become publicly available.
- Make or buy and **unnecessary cost**: there is risk of replication and of reinventing the wheel, thus wasting resources. A common solution should be the backbone in order to maximize the value added by new developments.
- **Lack of stability in terms of requirements.** This is a no-brainer for any complex software-intensive project. But that is not why it is mentioned here. Extra concerns should be raised because evolving requirements will be caused by evolving regulations. There are reasons to believe that new regulatory requirements will emerge, and this entails the risk that different supervisory and regulatory authorities will not have successfully harmonized their views and guidelines in the very near future – while the subject of course will remain a dynamic theme of debate and gradual improvement.
- While the end-to-end incident reporting environment will be fairly complex in its own right, it remains very important to avoid unnecessary overhead and variations in policy and regulations in different areas of the EU. For example, **fragmentation** of reporting requirements across Member States will increase the complexity of incident reporting by companies with cross-border activities. The cost and difficulty of complying with reporting requirements must be minimized from this perspective.

- Moreover, unnecessary fragmentation, duplication of effort and information flow will increase the **risk of abuse and attacks** on the reporting systems itself, and may thus even create an **additional risk to cyber resilience** itself.

### 6.6.3 European Digital Sovereignty

Several pieces of European regulatory legislation adopted in recent years have helped to improve cybersecurity capabilities and impose measures to prevent cyberattacks in key sectors.

We have already mentioned the importance, in the overall context of incident reporting, of cooperation and threat intelligence data sharing among the different stakeholders to improve the capacity and resilience of the European cyber environment and give a more rapid and efficient answer to cyber security threats.

Promoting European leadership in the digital field goes through a holistic approach to the threats, with the aim to protect assets efficiently, as a duty that must be guaranteed.

Incident reporting harmonization aims at adopting a unique standard requirement, as well as a unique taxonomy and methodology. The first goal is to speed up reporting to the Authority, but also to provide the opportunity of creating and managing uniform data to obtain a useful dataset to analyse, with the final goal of enhancing European cybersecurity resilience.

A tool that collects all the information about cyberattacks could be part of the path to reach digital sovereignty. Collecting useful information about the most common risks is the starting point for finding the most appropriate reactions and solutions. In this regard, data gathering necessary for incident reporting could be a part of building a trustworthy digital environment.

### 6.6.4 COVID-19 and Public Health Dimension

During the COVID-19 period, according to Interpol<sup>296</sup>, cybercriminals have made a major shift from individuals and SMEs to major corporations and critical infrastructure. Interpol projects that threat actors will increase their activities in the digital domain and develop more advanced and sophisticated *modi operandi*. Threat actors try to exploit the uncertainty and the impatience a situation has caused, by deploying online scams and phishing schemes themed in COVID-19, often impersonating government and health authorities. Opening such email attachments or links infects the used device, whether a computer or a smart device, opening a route to an organization's network. The threat actor could then capitalize on the established connection to achieve the goals of its operation. A key finding from the Interpol report is that Malicious Domains registrations increased by 569 per cent from February to March 2020. Whilst developing new tactics, techniques and procedures, threat actors also utilize previously proven methods, such as voice phishing impersonating an organization's IT-support.

In the report Organised Crime Threat Assessment, Europol ([Europol 2020] and [Europol 2021]) states it has followed attacks on organizations that play a key role in the supply chains of major financial institutions,

---

<sup>296</sup><https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19>

which are believed to be an attempt by the attackers to enhance pressure on the victim to pay the ransom. Later in the report, without naming the verticals, Europol states that some companies, hit by ransomware, negotiate behind the scenes with the ransomware actors to obtain a bigger discount from the ransom payment. Europol emphasizes that not reporting cases to law enforcement agencies will obviously hamper any efforts, as important evidence and intelligence from different cases can be missed. Europol reports<sup>297</sup> that in the European Money Mule Action (EMMA 6) operation, only a few COVID-19 related cases have been reported.

The FS-ISAC reported that from September 2019 to August 2020 there were a total of 91 ransomware incidents reported by the organization's members. The report highlights that cyberattacks on financial and banking institutions' supply chains, middleware fintech companies, have proven to be highly effective in circumventing the cybersecurity defences of financial institutions.

The National Cyber Security Centre of the UK reported<sup>298</sup> that, from 1 September 2019 to 31 August 2020, it handled 723 incidents, with around 200 related to coronavirus. The annual increase in incidents from the previous year was 20 per cent. The organization does not report business sectors or verticals in public.

During COVID-19, homeworking, or working from some other remote location has increased. The quick transition from on-premises work to remote work may have created a need to establish or increase the capacity of organizations' VPN services, remote access and authentication portals. The sudden but mandatory need may leave configuration errors in the services that threat actors try to exploit. Auditing of such services should be planned and implemented, and vendor patches promptly updated. Such services should be controlled and monitored according to the risk they introduce to the organization and its ecosystem. Both ENISA<sup>299</sup> and [Interpol 2020] recommend e.g. that organizations deploy multifactor authentication and implement network segmentation.

In a sectoral analysis report, ENISA<sup>300</sup> states that in the financial, banking and insurance sector it is hard to interpret the threat landscape, as different domains in the sectors may face entirely different cyber risks and threats. According to the report, the incident trends were stable. The report covers only the period between January 2019 and April 2020, a period when the global COVID-19 crisis had existed only for few months. Therefore, it can only be expected that the yearly report in 2021 will update the status of financial, banking and insurance sectors from the COVID-19 point of view.

Home and remote locations' networks and wireless access points equipment maybe acquired, set up, configured and monitored by a person having specialities in another area or domain. If the equipment is not provided or approved by the organization or controlled and monitored by it, the equipment may have vulnerabilities that cannot be patched, or its configuration may have unintended flaws. In attacking those, threat actors may gain a stepping-stone that brings them closer to the organization's and its ecosystem's networks. Such an attack path could be exploited to attack a financial institution's employee, or an employee

---

<sup>297</sup> <https://www.europol.europa.eu/newsroom/news/422-arrested-and-4%C2%A0031-money-mules-identified-in-global-crackdown-money-laundering>

<sup>298</sup> <https://www.ncsc.gov.uk/news/ncsc-defends-uk-700-cyber-attack-national-pandemic>

<sup>299</sup> <https://www.enisa.europa.eu/news/enisa-news/securing-smart-infrastructure-in-covid-19-pandemic>

<sup>300</sup> <https://www.enisa.europa.eu/publications/sectoral-thematic-threat-analysis>

of its service supplier. As of writing (3<sup>rd</sup> of December 2020), we found no indicators from publicly available reports that this specific attack path has been utilized.

Current publicly available sources do not indicate that the financial or banking sector has faced, at least dramatically, an increased number of cybersecurity incidents during COVID-19, even though they have increased overall.

The pandemic situation could have provoked shortages in the workforce, but thanks to the high technological level of the European financial institutions and the diffusion of the homeworking there have been no serious consequences and gaps in the provision of the service. Financial institution, in several countries, in 2020 helps Public Health with donations and other services. For example, in Italy, Intesa San Paolo<sup>301</sup> provided huge donations destined for public hospitals, for the construction of field and temporary hospitals to manage the emergency and has also financed the distribution of underwear to COVID patients recovered in hospital during lockdown.

### 6.6.5 Green Deal and Climate Change

The European Green Deal, an ambitious plan put forward by the European Commission to green the European Economy, has an impact on incident reporting solutions. “Europe needs a digital sector that puts sustainability and green growth at its heart.” However, digital solutions also tend to bring digital threats and the impacts of potential attacks become more and more severe. A fast response to a security incident and better coordination among the different stakeholders involved in the incident reporting procedure will help to minimize the effects of potential attacks.

Current incident reporting involves the generation of reports, which almost always have to be printed on paper. In order to provide an environment-friendly technology and reduce the need for wood to produce paper and the pollution emissions associated with paper manufacturing, printed reports could be replaced by a digital platform for mandatory incident reporting. Such a digital solution not only allows pollution to be reduced, but also provides additional functionality, such as aggregation and visualization of data related to cybersecurity incidents, which will become critical for the success of the Green Deal.

Such fast and environment-friendly incident reporting requires a cybersecure and trusted environment built on common and open building blocks that can be replicated and scaled across cities and communities in the EU.

Climate change may lead to an unexpected increase in the number of natural disasters, which, in turn, affect the Insurance sector (and consequently the Financial Services). Insurance companies often rely on historical

---

<sup>301</sup> refer to news published on the site <https://group.intesasanpaolo.com/it/sala-stampa/comunicati-stampa/2020>; for instance Comunicato Stampa 24 March 2020

data to plan financial reserves. Therefore, the unexpected number of incidents due to climate change might lead to a crisis in the Insurance sector. Such a risk makes insurance companies even more vulnerable to cyber-security threats: the adversaries are likely to exploit the situation by creating attack campaigns (e.g. phishing) against these companies.

Natural disasters might lead to damage to the physical protection of data centres and communication channels of financial institutions, or even their destruction. In such a case, the integrity of the highly sensitive financial data might be corrupted. Moreover, the lowered level of physical protection of communication channels and data centres makes it easier for adversaries to break the protection and inject sniffing devices into the sensitive networks that transfer financial data.

Furthermore, natural disasters could cause outages of power and/or Internet connection. In consequence, usual cyber security checks, e.g. those performed for every payment with a bank card, might be degraded to provide the ability for customers to still perform transactions (i.e. buy goods and pay for services). However, the lowered (or degraded) level of security for payments means an increased risk of cyber security incidents. The attackers might take advantage of the situation and steal money from bank accounts. All this, of course, may cause severe damage to the reputation of the financial institutions.

It has been observed over the last few years that the number of natural disasters, such as fires, hurricanes, or tsunamis, is increasing.<sup>302</sup> Such disasters caused by climate change could lead to physical damage of the infrastructure, which, in turn, might create opportunities for cyber criminals. Hence, climate change should be taken into account while planning business models for financial institutions. Moreover, the current cyber security strategies might not be sufficient to cover all the needs of the financial sector in the new environment. Novel methods addressing the rising risks of cyber security incidents in the financial sector should also be developed to address the changed nature of the cyber security threats caused by climate change.

### **6.6.6 Impact on Democracy**

One of the consequences of the harmonisation of incident reporting is the possibility of easy sharing of information about the attacks; this can help Threat Intelligence to cope with and manage attacks. In this sense, incident reporting helps to maintain a stable, reliable and credible financial system. The financial system is directly connected to a stable situation in a country, a situation present in a Democracy; the political situation of a region is crucial and has consequences for the financial environment, which is supported by a stable and free political situation.

Although it may appear that incident reporting in the financial sector has no clear or direct impact on democracy, it is a fact that most citizens maintain their money and savings deposited in a financial institution. To fight against cyber-attacks that go against these entities will help to keep safeguard these bank deposits. In this sense, not only reporting security incidents to the competent authorities, but also sharing this information with other financial institutions, will contribute to improving the security and reliability of these entities. In addition, as a chain reaction, avoiding this can lead to increased mistrust in

---

<sup>302</sup> <https://www.rutherfordsearch.com/blog/2021/09/climate-change-and-cyber-security-what-to-expect-in-financial-services>

these entities and a potential massive cash withdrawal, which could eventually cause economic instability and social tension.

## 6.6.7 Contributions to the EU CyberSecurity Strategy for the Digital Decade

### 6.6.7.1 Resilient infrastructure and critical services

One of the main areas of action included in the European Cybersecurity Strategy is to increase the level of cyber resilience of all relevant sectors, public and private, that perform an important function for the economy and society. In this sense, the European Cybersecurity Strategy [EC 2020A] establishes that the financial sector must “*strengthen digital operational resilience and ensure an ability to withstand all types of ICT-related*” (Information and Communication Technology) disruptions and threats.

The banking sector (credit institutions) and financial market infrastructures (operators of trading venues and central counterparties) are considered “*Essential Services*” by the reformed NIS Directive (Network and Information Systems Directive), as defined in Annex I of the Directive,<sup>303</sup> “*Essential Services: Sectors, subsectors and types of entities*”. Operational resilience of the financial sector is essential to ensure the resilience of the European infrastructure and critical services.

The research challenges of this vertical are related to the reporting of cyber incidents and operational security incidents that can affect the availability of a bank website or the availability of the financial entity’s business processes. Incident reporting is one of the main steps in the incident management and response process that needs to be followed in case of a security incident [ISO/IEC27035 2016].

Research and development initiatives related to incident reporting will help financial institutions to manage cyber incidents, so they will be an essential element to ensure the operational resilience of the financial entity and, therefore, the operational resilience of the financial sector.

First of all, the research priorities and the development of an incident reporting platform will facilitate the reporting of incidents and/or data leaks, as the incident reporting platform will assist financial institutions in the preparation, collection and reporting of the information related to a cyber incident in an easy and timely manner. The reduction of the complexity and administrative burdens related to incident reporting to the competent authorities will help the financial entity’s resources and efforts remain focused on restoring the services or systems affected by the incident, rather than on the development of the mandatory reports, which will finally contribute to the enhancement of cyber resilience in the financial sector. In this sense:

- Research in this vertical will facilitate the collection of information related to the security incident and/or data leak, establishing a data model and tools to gather all the information required to report the incident. The definition of a data model for collecting the required information for mandatory incident reporting, considering all applicable regulations to the financial sector, and the definition of an incident reporting workflow will help financial institutions to improve incident reporting processes and business continuity management processes, enhancing cyber resilience in the financial sector.

---

<sup>303</sup> [1\\_EN\\_ACT\\_part1\\_v3.docx \(europa.eu\)](#)

- Additionally, the fact that the information related to the security incident and/or data leak will be centralised in the incident reporting platform will have a positive impact on the incident management process, as it will be possible to analyse all the data stored in the platform to detect trends and determine the management and mitigation measures that have to be adopted after an incident has occurred, taking into account measures taken in previous similar incidents.
- Finally, all the information related to the security incident and/or data leak will be immediately available for all the areas or departments of the financial entity involved in the incident management and reporting process. This will facilitate collaboration between these areas and will have a positive impact on the incident management process, shortening the time needed to recover after the incident and to restore business processes and, therefore, enhancing the overall resilience in the financial sector.

On the other hand, the research initiatives in this vertical and the development of an incident reporting platform will provide a trusted and coordinated way of sharing cyber security data and promote a collaborative approach for incident information sharing, allowing financial entities to have access to relevant information applicable to their infrastructures, not only to quantify the actual risk level, but also to identify the most effective mitigation measures, leading to an improved cyber resilience in the financial sector. This will foster cooperation among public and private entities to fight against cyber-attacks and enhance cyber resilience.

#### **6.6.7.2 Building a European Cyber Shield**

This vertical does not directly contribute to this dimension.

#### **6.6.7.3 An ultra-secure communication infrastructure**

This vertical does not directly contribute to this dimension.

#### **6.6.7.4 Securing the next generation of broadband mobile networks**

This vertical does not directly contribute to this dimension.

#### **6.6.7.5 An Internet of Secure Things**

This vertical does not directly contribute to this dimension.

#### **6.6.7.6 Greater global Internet security**

This vertical does not directly contribute to this dimension.

#### **6.6.7.7 A reinforced presence on the technology supply chain**

Modern financial institutions increasingly depend on the software systems that manage their operations. Such software projects process highly confidential data and, therefore, must be certified for the correct functionality and absence of security vulnerabilities. Currently existing certification techniques are time consuming, and they typically require (manual) expert assessment of software to satisfy certain predefined criteria.

However, in the last decade, three major forces radically changed software projects [Pashchenko+ 2021]. First, the speed of software development has increased dramatically as a result of the widespread adoption of DevOps, and continuous integration and continuous delivery practices: several versions of a software project could now be released in a single day. Secondly, the role of centralised control on development teams has greatly reduced since software development teams have become self-organised and cross-functional due to the wide adoption of agile practices. Third, nowadays software projects heavily rely on the functionality developed within third-party projects. Indeed, such concepts allow developers to focus only on the differentiating feature of their project and then rely on third parties for everything else (e.g. cloud deployment, use of open frameworks, and so on). We observe that the key issue is not that it is free (although this is useful), but that it is in a state of constant change, and the changes are made by different people belonging to different organisations. Moreover, the nature of software development has changed: nowadays, software projects consist of both home-grown code and third-party components (free open-source software), while software developers not only develop their own code, but also consume the code from other projects. From a security perspective, the new situation brings two major challenges:

**Challenge 1 – Both internal and external sources of insecurity.** Current software security techniques mostly focus on in-house development. The root cause of software security problems is shifting from the development of home-grown software to the aggregation of third-party (external) components and libraries. In addition, each actor in the ecosystem may have different security and privacy practices. Security is no longer an internal force. In CI/CD, on any given sprint (e.g. a two-week development cycle), software developers pull in new FOSS libraries, the FOSS community produces security updates for those libraries, software developers make decisions that impact the (security) architecture of the systems, new features (and their associated security bugs) are deployed to the customers, and so on. This challenges software developers to take additional responsibilities for proper security assessment, security integration, and security maintenance of third-party components. For instance, secure coding skills might not be enough. If software developers refuse to take responsibility for the third-party components, the software that processes highly sensitive financial data might be affected by the security vulnerabilities introduced by those vulnerable components.

**Challenge 2 – From quality gates to continuous recertification.** As the organisation of software development activities has morphed into a fluid, fast-paced, and democratised process, the traditional separation into specialised units (e.g. front-end developers, functional testers) that worked under the oversight of software architects and security experts is no longer adequate.

Rigid “security gates” that apply heavyweight security techniques (such as architecture risk analysis, code verification, etc.) rely on the availability of stable artefacts at fixed points in the development process and assume the supervision of a few highly-skilled security specialists.

Such a centralised model needs to evolve to sustain fast-paced software development<sup>304</sup>: “If the software security industry is going to make a meaningful impact, then everything has to be as easy as humanly possible for both the developers and users of software.”

Hence, security assurance might greatly benefit from embedding precautions into the development and operation pipeline, in the form of lightweight, intelligent, fully- or semi-automated techniques that can be executed at scale to provide screening tests of security-relevant events (e.g. importing an open-source library that requires patching, deploying a container, etc.). These techniques enable an incremental (thus

---

<sup>304</sup> J. Viega, “20 years of software security,” *Computer*, vol. 53, no. 11, pp.75–78, 2020

continuous) re-certification of financial software and their outcome can guide the application of further, in-depth analysis that is more focused and may require expert intervention.

#### **6.6.7.8 A Cyber-skilled EU workforce**

This vertical does not directly contribute to this dimension.

#### **6.6.7.9 EU leadership on standards, norms and frameworks in cyberspace**

The EU plays a prevalent part in the international area and fulfils the role of an influential subject in acting like a leader.

A prominent challenge for the future of incident reporting is the harmonisation of the regulatory framework adopted. A leader is crucial to define the path for fulfilling the goal. The EU should take part in the process, also thanks to its role in determining rules for the members. The role held by its supervisory authorities makes it possible to know closely the needs that must be met by the legislation, but at the same time allows the EU to have a leading and conscious role in determining the rules.

Identifying a set of information that the authorities need to receive to be able to understand the seriousness of the incident, at least at the European level, is the first step in building a common understanding of the risks.

The common view, required by a relevant institution, should pave the way to new common standards for the whole European system.

To promote financial stability in the EU and enhance cyber resilience, several steps need to be encouraged:

- Harmonisation (in taxonomy, methodology, processes) to facilitate the reporting of incidents to the competent authorities and to simplify compliance with the rules at national and European level;
- Promotion of collaborative information sharing about the incident suffered—crucial in detecting the trends and the methodology of attack so as to manage the mitigation measures;
- Facilitating the sharing of information, comparing and contrasting attacks, so that a suitable solution may be adopted promptly.

The lack of harmonisation in the actual incident reporting process is a reality that all European financial institution has to face. The tool in development in this vertical, a data model for helping the collection of information for incident reporting in the financial sector by providing assistance in completing the documents required, could be the first step in standardising the process.

#### **6.6.7.10 Cooperation with partners and the multi-stakeholder community**

The research initiatives in this vertical and the development of an incident reporting platform will provide a trusted and coordinated way of sharing cyber security data, and will promote a collaborative approach for incident information sharing, allowing financial entities to have access to relevant information applicable to their infrastructures, not only to quantify the actual risk level, but also to identify the most effective mitigation measures, leading to improved cyber resilience in the financial sector. This will contribute to the emergence of a multi-stakeholder community and will foster cooperation among public and private entities to fight against cyber-attacks and enhance cyber resilience in the financial sector.

### 6.6.7.11 Strengthening global capacities to increase global resilience

European leadership in the digital field goes through a holistic approach to the threats, aiming to protect assets efficiently. In the EU, the safety of cyberspace must be guaranteed so that all members will feel protected and so free to grow and develop. European companies have suffered several cyberattacks and threats in this field, so they will benefit from a holistic protective system.

Cyberattacks and threats to the financial system are growing rapidly, while third-party service providers are now also under attack, often being less protected, so everybody will benefit from a holistic protective system. Consequently, in the current situation it is necessary to increase cyber-security resilience in the EU from a global perspective that integrates all the stakeholders involved.

In the same way, enhancing cyber resilience to promote financial stability in the EU, but also in the whole financial system, is the first step towards a global and thriving global market. A cyber-attack-resilient environment protects against economic shock, or at least makes it less likely. Financial institutions play an important role in protecting the cyber resilience of the financial system, but they need assistance in doing so.

Incident reporting can be an effective means of protecting the overall financial system, by making authorities aware of incidents and issues that could impact the system. Depending on how authorities use the information received, it can also help others to recover faster or avoid becoming a victim of that type of attack. Incident management can take advantage of the sharing of information about how to cope with some types of incidents. The main issue is the types of information to share. In particular, regarding very sensitive data, the challenge is to find the right balance between providing useful information to others without spreading too much information about oneself. Nevertheless, to increase the global resilience a closer cooperation is required, in compliance with the legitimate right not to disclose sensitive information that can make the victim even more attackable.

### 6.6.8 Sector-specific Dimensions

The financial sector is a highly regulated sector. The existing fragmentation and the need to report to different authorities and supervisors create additional regulatory and operational burdens.

The current cyber incident reporting framework is characterized by a high degree of fragmentation, with different taxonomies, thresholds, timing, templates, and information requirements. This fragmentation creates increasing complexity and administrative burdens for financial institutions, adding costs and diverting resources from where they are most needed after a cyber-incident occurs (limiting the impact of the incident).

Moreover, fragmentation of reporting requirements across Member States increases the complexity for companies with cross-border activities to comply with reporting requirements and could even pose a risk to cyber resilience. Harmonization of requirements regarding incident reporting at a European level is an essential element in the fight against cybercrime, especially in the case of incidents affecting several Member States.

The research roadmap in this vertical will foster cooperation among public and private entities to fight against cyberattacks and enhance cyber resilience.

The mandatory reporting requirements are particularly complex in the financial market, since a cyberattack on a financial institution could cause important and disruptive consequences in the financial sector, undermining the whole sector. For this reason, combatting cyberattacks is a priority. The attacks become more sophisticated every time, so the combatting methods must be efficient, ready and trustworthy.

A financial sector aware of the risks is more collaborative in combatting the common threat by working together. Sharing information on cyberattacks suffered is part of the path leading to the final result of achieving a more secure sector.

### 6.6.9 Summary of the dimensions and impact on the Roadmap

Previous sections have analysed how different dimensions (such as green and climate dimensions, COVID-19 and sector-specific dimensions) impact on incident reporting in the financial sector and/or how this vertical can contribute in some way to those dimensions. As a summary, given the indirect impact it can have on different dimensions for citizens, the importance of fighting and preventing cyber-attacks against financial institutions can be highlighted, not only for its economic impact, but also to increase the reliability and trustworthiness of users in these institutions. This links directly with the need to improve the methodologies and tools used in this vertical for efficient and rapid information gathering, and reporting information about the cyber-incidents detected to the competent authorities. To foster collaboration by sharing threat intelligence data between stakeholders in the financial sector is also a related key point. On the other hand, another recurrent topic in the analysis is the disparity and number of different existing regulations that require mandatory incident reporting, as that applies to the financial sector. This has a negative impact in the vertical because this fragmentation and lack of unification in the requirements implies complexity, which translates into an increase in the costs and time spent on incident management. Consequently, the results of the analysis of these dimensions have helped us to better identify which challenges and developments we need to include in the roadmap.

### 6.6.10 Challenge 1: Lack of harmonization of procedures

The first challenge that emerges from the need of compliance with multiple regulations and supervisory authorities at different levels (local, national, European, industry) is the fact that each of them has its own set of procedures. This implies, for example, the definition of a common incident taxonomy and incident reporting workflow, taking into account all applicable regulatory requirements.

#### Specific Research goals:

- ***Definition and development of a mandatory incident reporting workflow for the financial sector***, based on the procedures and regulations that applies to the financial sector at different levels related to incident reporting.
- ***Definition of a data model for collecting the information required for the mandatory incident reporting in the financial sector***, considering the data required in the reports for the different applicable regulation and trying to unify them in a common data model.
- ***Definition of a common severity event classification procedure in the financial sector***, that can be applicable to the different thresholds and criteria defined by each regulatory framework depending on the type of security event.

#### JRC Cybersecurity Domains:

- Incident Handling and Digital Forensics
  - Incident analysis, communication, documentation, forecasting (intelligence-based), response, and reporting;
  - Resilience aspects;
  - Citizen cooperation and reporting;
  - Coordination and information sharing in the context of cross-border/organizational incidents.
- Security Management and Governance
  - Risk management, including modelling, assessment, analysis and mitigation;
  - Managerial aspects concerning information security;
  - Standards for information security;
  - Governance aspects of incident management, disaster recovery, business continuity;
  - Compliance with information security and privacy policies, procedures, and regulations.
- Human Aspects
  - Enhancing risk perception;
  - Automating security functionality;
  - Privacy concerns, behaviours, and practices.
- Legal Aspects
  - Cybersecurity regulation analysis and design.

#### JRC Sectorial Dimensions:

- Financial

#### JRC Technologies and Use Cases Dimensions:

- Information systems

### 6.6.11 Challenge 2: Facilitate the collection and reporting of incident and/or data leaks

A second challenge for mandatory incident reporting emerges during the process of gathering all the information required about a security incident. This includes the identification or provision of incident management and response tools or technologies that help the users in the preparation, collection and reporting of the information related to a detected cyber incident in an easy and timely way.

#### Specific Research goals:

- *Definition of questionnaires for data collection for mandatory incident reporting in the financial sector*, that can be used to facilitate the gathering of the information required to populate the mandatory reports according to the different templates defined for the applicable regulations.
- *Enforcement of the mandatory incident reporting workflow and support for managerial judgement*, to help the users to follow the required procedures and ensuring there is an approval at specific steps before continuing e.g. with the preparation of the reports or the notifications.
- *Preparation of reports for mandatory incident reporting in the financial sector*, based on the information collected through the questionnaires and considering the templates provided by the different financial regulatory frameworks for mandatory reporting.

### JRC Cybersecurity Domains:

- Incident Handling and Digital Forensics
  - Incident analysis, communication, documentation, forecasting (intelligence-based), response, and reporting;
  - Resilience aspects;
  - Citizen cooperation and reporting;
  - Coordination and information sharing in the context of cross-border/organizational incidents.
- Security Management and Governance
  - Risk management, including modelling, assessment, analysis and mitigation;
  - Managerial aspects concerning information security;
  - Standards for information security;
  - Governance aspects of incident management, disaster recovery, business continuity;
  - Compliance with information security and privacy policies, procedures, and regulations.

### JRC Sectorial Dimensions:

- Financial

### JRC Technologies and Use Cases Dimensions:

- Information Systems

#### 6.6.12 Challenge 3: Promote a collaborative approach for sharing incident reports to increase risk quantification, mitigation and thus overall cyber resilience

The third challenge identified arises from the need for better cooperation among public and private entities to fight against cyber-attacks and enhance cyber resilience. To achieve this goal, it is necessary to provide a trusted and coordinated way of sharing cyber security data that fosters collaboration and allows the users to have access to actually relevant information applicable to their infrastructures to quantify the actual level of risk, identify the most effective mitigation and therefore improve its cyber resilience.

#### Specific Research goals:

- *Improve trust for threat intelligence sharing*, through the usage of trustworthy APIs for threat intelligence sharing and a distributed security framework.
- *Qualification of Indicators of Compromise to provide reliable and actionable threat intelligence data*, using a multi-dimensional trust model for reliable CTI-sharing and analysing data received from a threat intelligence data sharing platform and correlating it with information about the infrastructure of a specific organization and incidents already registered in the incident reporting platform.
- *Quantification of risks (and effective risk reduction of mitigations)* by using the indicators and the incident data to define the concrete, experimental effects in terms of risk reduction of various mitigations in the light of different measures available to stakeholders (mitigations, transfer and cyberinsurance, risk acceptance and communication, etc.). This is particularly relevant for the analysis of incidents caused by advanced persistent threats (APTs).

### JRC Cybersecurity Domains:

- Incident Handling and Digital Forensics
  - Incident analysis, communication, documentation, forecasting (intelligence-based), response, and reporting;
  - Resilience aspects;
  - Citizen cooperation and reporting;
  - Coordination and information sharing in the context of cross-border/organizational incidents.
- Trust Management and Accountability
  - Semantics and models for security, accountability, privacy, and trust
  - Trust management architectures, mechanisms and policies
  - Trust and privacy
  - Identity and trust management
  - Trust and reputation of social and mainstream media
  - Reputation models.
- Human Aspects
  - Enhancing risk perception;
  - Automating security functionality;
  - Privacy concerns, behaviours, and practices.

### JRC Sectorial Dimensions:

- Financial

### JRC Technologies and Use Cases Dimensions:

- Information Systems

## 6.7 Mapping of the Challenges to the Big Picture

First, there is a need in the incident management and response process to facilitate the collection of the information about the security incidents and the preparation of the mandatory reports that need to be sent to the different supervisory authorities that applies to the financial sector (challenge 2). And it needs to be adaptable enough to support the different incident reporting workflows and procedures established due to the lack of harmonization among the different regulatory frameworks (challenge 1). Finally, it is necessary to provide mechanisms and tools that enhance the trustworthiness and reliability of the current threat intelligence data sharing platforms so they help to boost the cooperation among stakeholders and the overall cyber resilience across Europe.

## 6.8 Methods, Mechanisms, and Tools

This section describes the mechanisms and tools to address the main functionalities included in the challenges described in previous section, indicating if they will be covered by some asset developed in WP3 or additional open source tools or development need to be used.

### 6.8.1 Incident Data Collection

The first step in the workflow envisaged for incident reporting is the gathering of all the data regarding the incident that meets Challenge 2, in particular within the financial sector. This includes the collection of three types of information: general data (e.g. the name of the legal entity affected, the event timeline, the impacted areas entailing EU regulatory requirements for incident reporting or the incident status), information that identifies the type of incident (depending on whether it is a cyber-incident, an operational security incident, or both), and specific information to assess the need for mandatory incident reporting. Taking into account that for each European regulatory framework (such as the ECB cyber incident reporting framework, GDPR, NIS Directive or eIDAS regulation) the procedure for mandatory reporting is different and the set of information to be included in the report is also diverse, the challenge, in this sense related to Challenge 1, is to provide a tool for harmonising and simplifying the procedures for data collection when an incident takes place. A friendly and easy way will be offered to the user to perform this phase of the incident reporting workflow, through questionnaires and a graphical interface. Depending on the regulatory framework selected, the questions presented to the user need to be different and, in some cases, may be based on previous answers. However, currently there are no tools being developed in WP3 or open-source solutions to meet this type of need for smart data collection. To support incident data collection included in Challenge 1 for harmonisation of mandatory incident reporting, a common data model for incident reporting has been defined as suitable for registering the information required by the different regulations. Through the use of different catalogues, in the data base a single entity contains all the potential options that could be selected for the same piece of information (e.g. root cause of the incident). Later, in the generation of the reports, the stored data are mapped to the concrete options of a specific regulation. There are also some tools that can help the user on the incident management team to understand the incident's severity and its extent for some specific types of cyber incidents, as a step in the data collection for incident reporting; however, the collection of the information required for each incident report to be compiled should be performed manually. These WP3 tools are HADES, specifically to analyse malware samples, and JUDAS, to analyse users and devices. Open-source incident management and response tools were analysed during Roadmap 1 to check whether they can support the incident management teams in dealing with Challenge 2, and to what extent. Finally, the open-source packages TheHive<sup>305</sup> and Cortex<sup>306</sup> have been chosen to cover this functionality, which is complemented by the information collected through the AIRE asset GUI, where questionnaires to retrieve additional data about incidents for mandatory reporting have been included, together with information about the regulatory frameworks.

### 6.8.2 Incident Impact Assessment (and transferability to other organization)

Once all the information related to the incident has been collected, it is necessary to quantify the incident according to the different EU mandatory incident reporting regulatory requirements. This is linked with Challenge 1, since each regulatory framework establishes its own criteria and thresholds to categorise the severity of the incident reported. In WP5, a security incident classification methodology was analysed that identifies the need for mandatory reporting to the competent authorities, considering the information collected about the incident and applying the appropriate thresholds and criteria defined under each set of requirements. However, no tool has been developed in WP3 to automate the evaluation of the algorithms defined using the data collected and the different thresholds and criteria, and to suggest whether there is a

---

<sup>305</sup> <https://thehive-project.org>

<sup>306</sup> <https://github.com/TheHive-Project/Cortex>

need to report for each of the EU regulatory frameworks considered. Nor does any open-source solution seem capable of covering this automatic step of harmonisation and facilitation of incident reporting. Consequently, this functionality of the incident reporting platform has been included in Roadmap 3 through the implementation in WP5 of a Responder<sup>307</sup> that can be invoked from the GUI of the open-source tool TheHive. However, this event classifier is not customisable and does not implement a classification methodology. It only analyses a predefined set of criteria and thresholds as established by the current regulations supported by the demonstrator, based on the information registered about the incident.

Further, as observed in Challenge 3, the ability to have an indication of the possible impact is important for the qualification of indicators and the quantification of risks. The risk can be quantified by simulating the adversaries, starting from the information related to the incidents. Appropriate and measurable metrics should be employed to quantify the likelihood of being compromised and the overall risk. In the case of different incidents, the risk could be described through relative metrics based on a base case incident to determine the reduction or increment of risk for the different scenarios. During Roadmap 3, this possibility will be analysed through the integration in the demonstrator of WP3 assets related to the analysis of threat intelligence data.

### 6.8.3 Incident Reporting

Another consequence of the lack of harmonisation (Challenge 1) among the different European regulatory frameworks is that the format defined to communicate an incident (e.g. if it needs to be prepared in an Excel or Word document with a predefined template) and the channels to be used (e.g. sending an email to a specific address) can be different. The timings are also different depending on the regulation considered and on the severity of the incident to be reported. This disparity in procedures makes it difficult and sometimes time-consuming to address all the mandatory reporting in a timely way and may discourage the entities from cooperating with a view to enhancing global cyber resilience. Additionally, the mandatory incident reporting procedures tend to enforce an incident reporting workflow where not all phases can be carried out automatically, but require the 4-eyes principle to avoid accidental reporting. Consequently, it is necessary to develop a tool to deal with these functionalities of workflow enforcement and data conversion, to support the incident reporting team in the preparation of the mandatory incident reports, according to the different templates based on the data collected, and the notification of the supervisory authorities via the specified communication channels. The asset AIRE (Atos incident reporting engine) has been developed in the context of T3.5 to deal with these challenges.

### 6.8.4 Collaborative incident sharing platform

In the context of task 3.4, different tools based on the MISP<sup>308</sup> open source threat intelligence platform and open standards for threat information sharing are available to deal with the challenges related to collaboration and voluntary information sharing. This will be included mainly in Challenge 3, as described in the previous section, although it also covers some points of Challenge 2. A variety of research has been

---

<sup>307</sup> <https://github.com/TheHive-Project/CortexDocs/blob/master/api/how-to-create-a-responder.md>

<sup>308</sup> <https://www.misp-project.org/>

carried out to improve the security of data exchanged through the MISP platform, enhancing and extending its security features, and trust models have been analysed and developed to encourage institutions or organisations affected by a security incident to share sensitive and threat-related information with CERT/CSIRTS, companies or other related entities. In particular, these tools are MISP++, Reliable Cyber-Threat Intelligence Sharing (Reliable-CTIs) and the Threat Intelligence Integrator (TIE).

Table 5: Challenges identified in the Incident Reporting Vertical and Tools needed to address them

Challenge	Tools required for	Tools contemplated for Incident Reporting	Tools/Methods that need to be addressed
Challenge 1	Incident management, workflow enforcement and event classification.	AIRE - Atos Incident Reporting Engine (D3.1, Section 5.4)  Event Classifier Responder (integrated with TheHive)	Design of data model for data collection of information required for mandatory incident reporting in the financial sector and development of an Incident Register database. Design and implementation of workflow for mandatory incident reporting in the financial sector. Adaptation/extension of the open source incident management tool TheHive to support mandatory incident reporting workflow in financial sector and event classification.
Challenge 2	Data collection, incident management and reporting	AIRE - Atos Incident Reporting Engine (D3.1, Section 5.4), HADES – Automatic analysis of malware samples and JUDAS (D3.1, Section 5.3)	Adaptation of the open source incident management tool TheHive and integration with HADES, JUDAS and AIRE for data collection and mandatory incident reporting workflow enforcement. Generation of reports based on information collected according to the different regulations in the financial sector.
Challenge 3	Threat intelligence data sharing	TATIS - Trustworthy APIs for enhanced threat intelligence sharing, Reliable-CTIs - Reliable Cyber-Threat intelligence sharing, TIE - Threat Intelligence Integrator (D3.1, Section 5.3)	Mechanisms to improve trustworthiness and reliability for threat intelligence data sharing using MISP and qualification of IoCs to improve actionability.

## 6.9 Roadmap

### 6.9.1 Short-term plan

The activities to be completed until the end of the project related to this vertical can be summarised in the following points:

- Consolidation of the incident reporting platform, extending the capabilities of the demonstrator to support the generation of the different reports (initial/intermedium/final) required for the following regulations: incident reporting for significant institutions under the ECB/SSM Framework, incident reporting for Payment Service Providers under PSD2, incident reporting for Operators of Essential Service under the NIS Directive, incident reporting for Target2 participants, incident reporting for Trust Service Providers under eIDAS regulations, and notification of Personal Data Breaches under the GDPR.

Integration of the demonstrator with a MISP platform and WP3 assets to provide the platform with trustworthy threat intelligence data sharing capabilities and mechanisms to determine and quantify the reliability and actionability of the information received

## 6.9.2 Beyond the end of the project plan

### 6.9.2.1 Security 2025

The following bullets summarise the problems related to incident reporting in the financial sector vertical that we would like to see solved by 2025:

- Automatic certification and re-certification of financial software given the current nature of fluid and fast-paced software development, where software projects are not created by a single organisation, but rather collected from various (often free open-source software) components. In this respect, novel security methods need to be developed that support the automatic certification and re-certification of only the changed components of software projects. Such methods could rely on machine learning techniques to quickly assess the changes in a software project and, if needed, request the intervention of traditional software verification techniques or human experts.

### 6.9.2.2 Security 2030

The following bullets summarise the problems in the incident reporting in the financial sector vertical that we would like to see solved by 2030:

- The definition of standards and taxonomies (at least at European level) that allows the classification and categorisation of all the information available about a security incident during an investigation, together with unification of the notification procedures that need to be followed, independently of the different regulatory frameworks. Coordination and better collaboration among the different stakeholders and supervisory authorities is necessary.

## 6.9.3 Milestones

By the end of the project, the vertical is expected to reach the following milestones:

- Testing and validation of the incident reporting platform demonstrator, which will be documented in the deliverable D5.6.
- Incident reporting platform demonstrator connected to a MISP instance to share threat intelligence data about security incident reported with CONCORDIA project.

## 6.10 Summary

This section focused on the reporting of security incidents in the financial sector. As it was described, the diversity and fragmentation of the requirements and procedures related to the mandatory reporting of security incidents included in the different regulatory frameworks that applies to the financial sector and the participation of many different stakeholders in the incident reporting process, lead to the need (i) for a common methodology and taxonomy, and (ii) for the harmonization and automation in the data collection and incident reporting procedures.

A brief SWOT Analysis in section 6.6.2 highlighted that the EU has the awareness, understanding, and talent pool to have the leadership in building a collaborative incident reporting platform for the financial sector. However, this is not an easy task and the implementation and deployment of this platform may encounter some limitations and threats such as (i) the high cost, (ii) the inherent complexity due to regulatory fragmentation and lack of stability in terms of requirements, (iii) the lack of available off-the-shelf technology, and (iv) the operation overhead in management. Anyway, we foresee interesting opportunities in this vertical not only to improve the incident management processes and reduce efforts to the organizations, but also to enhance the overall threat intelligence data sharing and go towards a European system more resilient and able to contrast efficiently cyber-attacks.

In this sense, the incident reporting harmonization and the availability of a collaborative platform for the collection and sharing of relevant information about cyber-attacks in the financial sector can help to promote the European leadership in this area and contribute to the European Digital Sovereignty (see section 6.6.3).

We have also analysed how the COVID-19 pandemic has impacted in this vertical but, although the focus of cyber-attacks have moved to major corporations and critical infrastructure and there is an overall increase in the number of attacks and in the attack surface, at the time of this writing the available current public sources found do not show a significant increase of the cybersecurity incidents affecting the financial sector during the first period of the pandemic.

Considering the priorities rising for the financial sector specific dimension (see section 0), we have identified the following major research areas:

- Previous sections have analysed how different dimensions (such as green and climate dimensions, COVID-19 and sector-specific dimensions) impact on incident reporting in the financial sector and/or how this vertical can contribute in some way to those dimensions. As a summary, given the indirect impact it can have on different dimensions for citizens, the importance of fighting and preventing cyber-attacks against financial institutions can be highlighted, not only for its economic impact, but also to increase the reliability and trustworthiness of users in these institutions. This links directly with the need to improve the methodologies and tools used in this vertical for efficient and rapid information gathering, and reporting information about the cyber-incidents detected to the competent authorities. To foster collaboration by sharing threat intelligence data between stakeholders in the financial sector is also a related key point. On the other hand, another recurrent topic in the analysis is the disparity and number of different existing regulations that require mandatory incident reporting, as that applies to the financial sector. This has a negative impact in the vertical because this fragmentation and lack of unification in the requirements implies complexity, which translates into an increase in the costs and time spent on incident management.

Consequently, the results of the analysis of these dimensions have helped us to better identify which challenges and developments we need to include in the roadmap.

- Challenge 1: Lack of harmonization of procedures
- Challenge 2: Facilitate the collection and reporting of incident and/or data leaks
- Challenge 3: Promote a collaborative approach for sharing incident reports to increase risk quantification, mitigation and thus overall cyber resilience

This roadmap also includes (see section 6.6.6) the following: how climate change can impact on the financial sector, and in particular on the reporting of security incidents in this sector; the impact of this vertical on democracy (see section 6.6.7); and how the incident reporting platform demonstrator can contribute to the EU CyberSecurity Strategy for the Digital Decade (see section 6.6.8).

Finally, we have tried to identify problems related to incident reporting in the financial sector that we would like to see solved by 2025 and by 2030.

The final goal of the work will be the harmonisation of incident reporting in the financial sector, at least at a European level, to facilitate reporting but also the handling of incidents and the resilience of the European cyber environment, to provide a more rapid and efficient answer to the new cyber security threats.

## 7 Maritime Transport

### 7.1 The Big Picture

Maritime Transport is a complex activity, engaging all the structures, modes and equipment required for the carriage of passengers or cargo shipping via sea, that constitutes the shipping trade (seaborne), supported by vessel transportation. Maritime transport is seen as the driving force of international trade and the backbone of globalization. According to the NIS Directive [NIS DIRECTIVE 2016], maritime transport has been defined as “inland, sea, and coastal passenger and freight water transport companies”.

Concerning the EU economy, maritime transport is considered a crucial activity, enabling import and exports of goods, supply of energy, facilitating intra-EU trade (transactions within the EU) and the transport of passengers and vehicles [EC 2018]. The cornerstones of the maritime transport and logistics industry are port communities. Vessels are the maritime transport means for conducting seaborne transport operations. Autonomous ships are seaborne vessels that transport freight over navigable waters without or with limited human interaction. Maritime transport enfold a composite set of stakeholders to carry on land–sea connection (i.e. port authorities, port terminal operators, service providers, other involved entities, such as local agents, ship owners, ship agents, carrier agents, marine underwriters, ship-brokers and other authorized bodies, such as customs, port police, and coast guard). Maritime stakeholders are considered the key players throughout the global economy of transport and intermodal logistics operating cyberphysical, complex and heterogeneous systems and interacting through cyber and physical transitions to support maritime transport services. The maritime transport services as a whole drive the implementation of supply chain processes across the maritime transport sector. Indicative maritime transport services are passenger transport, LNG (liquefied natural gas) transport, container cargo service, dry and bulk cargo service, route planning and vessel traffic service. Standardization bodies and policy makers of the Member States have recognized a top list of the maritime transport services concerning their criticality within the maritime transport supply chain and the damage they could cause to the maritime ecosystem in view of their interruption. The maritime transport critical services are presented in section 7.3.

Maritime transport services are implemented through maritime critical information infrastructures. Indicative maritime transport infrastructures are Information and Communication Technology (ICT) systems, Automatic Identification System (AIS), Supervisory Control and Data Acquisition (SCADA) system, Port Community System (PCS), Terminal Operating System (TOS), Vessel Traffic Services, Ship Information System (SIS), Electronic Chart Display and Information System (ECDIS), Electronic Data Interchange (EDI) systems and ERPs. The incremental evolving of technology in accordance with the spread of automation and digitalisation on maritime transport operations has raised the need to look for strategies, methods and tools that can adequately secure the dynamic environment of maritime transport; the involved operators, the critical information infrastructures (of ports and vessels) that function and their corresponding communications.

Considering the high impact of maritime transport on the EU economy, it is extremely important to invest in the protection of critical EU maritime infrastructures in order to maintain their security and thus ensure the sector’s preparedness and resilience. The big picture of maritime transport is presented in Figure 12 and is further explained and analysed in the following sections.

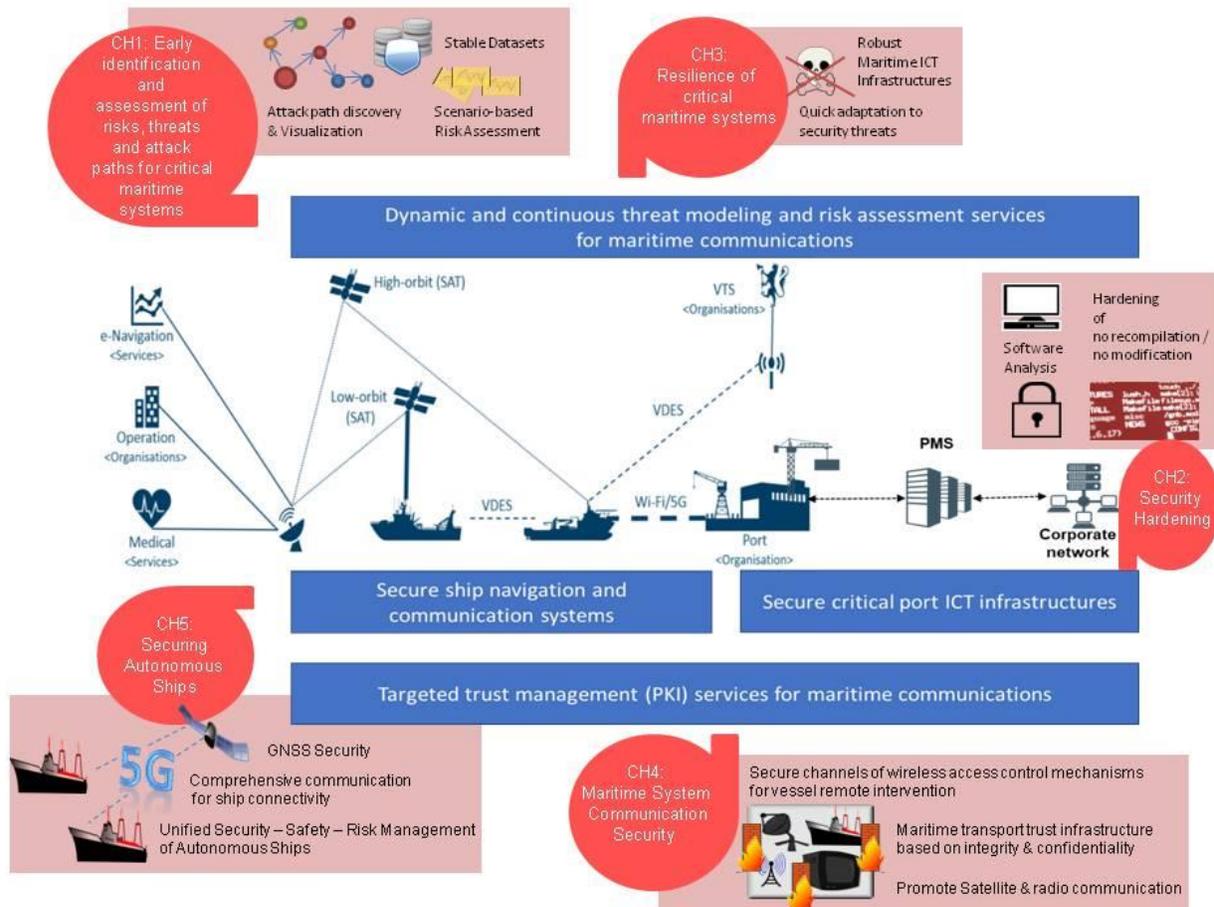


Figure 12: The big picture of a resilient EU maritime transport ecosystem

## 7.2 Overview

The maritime transport sector is a dynamic environment that involves a variety of interactions between cyber-physical systems and people. Such complex structures provide a vast attack surface, where many attack paths occur because of various causes ranging from software vulnerabilities to human error. To identify the cybersecurity challenges in the maritime transport sector, we must first identify the systems that are at stake, the attackers that threaten the critical maritime systems and the potential impact of security incidents.

Although the identification of the critical maritime ICT infrastructures used to be a trivial task, this is not the case in today’s maritime ICT ecosystem. Nowadays, maritime systems are highly automated systems. Instead of being isolated systems, the deployment of new technologies such as the internet of things (IoT) has given them advanced computation and communication capabilities, turning them into highly interacting and interconnected systems. Maritime navigational systems, collision avoidance systems, cargo management systems and infotainment systems are some examples of modern IoT-enabled maritime ICT systems. On top of that, the maritime transport environment is inherently hostile and vulnerable to physical threats. Recent piracy incidents have shown that modern pirates and mobsters are capable of utilizing

advanced hacking techniques and launching combined cyber-physical attacks against ships and/or port installations. Thus, modelling the cyber security threats and assessing the relevant cyber security risks is an open problem.

One side-effect of the increased interconnectivity of maritime ICT systems is their increased exploitability level. Since the use of legacy systems is very common in maritime transport, in many cases, updating and patching security vulnerabilities is hard to enforce. Obviously, the interconnectivity of potentially vulnerable systems that are not properly isolated creates new opportunities for the attackers to combine different vulnerabilities found in different systems. This may enable remote hackers to extend their attack vectors, turning locally exploitable vulnerabilities to remotely exploited ones by combining different vulnerabilities found in different systems. For example, a vulnerability found in an internet-enabled non-critical service, may be used by skilful adversaries as a remote entry point to move laterally inside the ship network and eventually to take over a critical legacy system. Dealing with such attacks may require that various layers, such as the communication layer and the system layer, be properly secured. Setting up secure and trusted communications, properly hardening maritime systems at the software level and assuring the resilience of critical maritime systems, such as those utilized in autonomous ships, are some of the relevant open research problems.

In order to set up a research roadmap for maritime transport security, we will follow a risk-based approach. By utilizing various existing taxonomies, we will identify the critical maritime assets, services and systems. By studying recent security incidents, we will identify the emerging threat actors and threat events against critical maritime transport systems, having in mind the potential impact of such security events. Then, we will identify existing tools, methods and mechanisms that may be utilized, both within and outside the scope of the CyberSecurity4Europe project, to properly secure the critical maritime systems. Based on the description of the current threat landscape and the existing security tools, we will identify the major research challenges in securing maritime transport and we propose a research roadmap towards this direction.

## 7.3 What is at stake?

Throughout the following subsections various taxonomies will be adapted, combined and presented in order to illustrate the critical cybersecurity aspects of this vertical. Mapping the threats that occur in this sector requires the utilization of taxonomies on (i) critical maritime assets and services, (ii) threat events, (iii) threat actors and (iv) impact of threats. Those taxonomies are used in order to map the critical assets and services presented beforehand.

### 7.3.1 What needs to be protected?

Multiple organizations have expressed their point of view as to which assets and services should be considered critical in the maritime sector through various taxonomies. In order to present a perspective that takes into consideration every possible asset and service that might be of high value in the current vertical, taxonomies from multiple vendors are integrated, adapted and extended. The purpose of the resulting taxonomy would be not only to assess the important assets of maritime companies and organizations, but also to examine components that might not seem to hold a high value when placed under scrutiny on their own. Although the individual value those assets hold might be low, such components have the potential to act as entry points to attack critical services when they are examined as a part of an interconnected system. Three popular taxonomies are taken under consideration.

The Member States have already identified the following critical essential services in water transport [IMO 2003]:

- Passenger transport
- Transport of freight and dangerous goods
- Route planning
- Ship maintenance
- Ship accommodation
- Management of water transport infrastructure
- Information, accommodation, screening, boarding of passengers
- Vessel traffic services

ENISA is providing another asset taxonomy [ENISA 2019] for critical maritime assets, which is illustrated in Figure 13. The operators of the services (ports, port authorities, maritime supply chain providers) need to become compliant with NIS and protect all their physical and cyber assets used in the provision of the critical services.

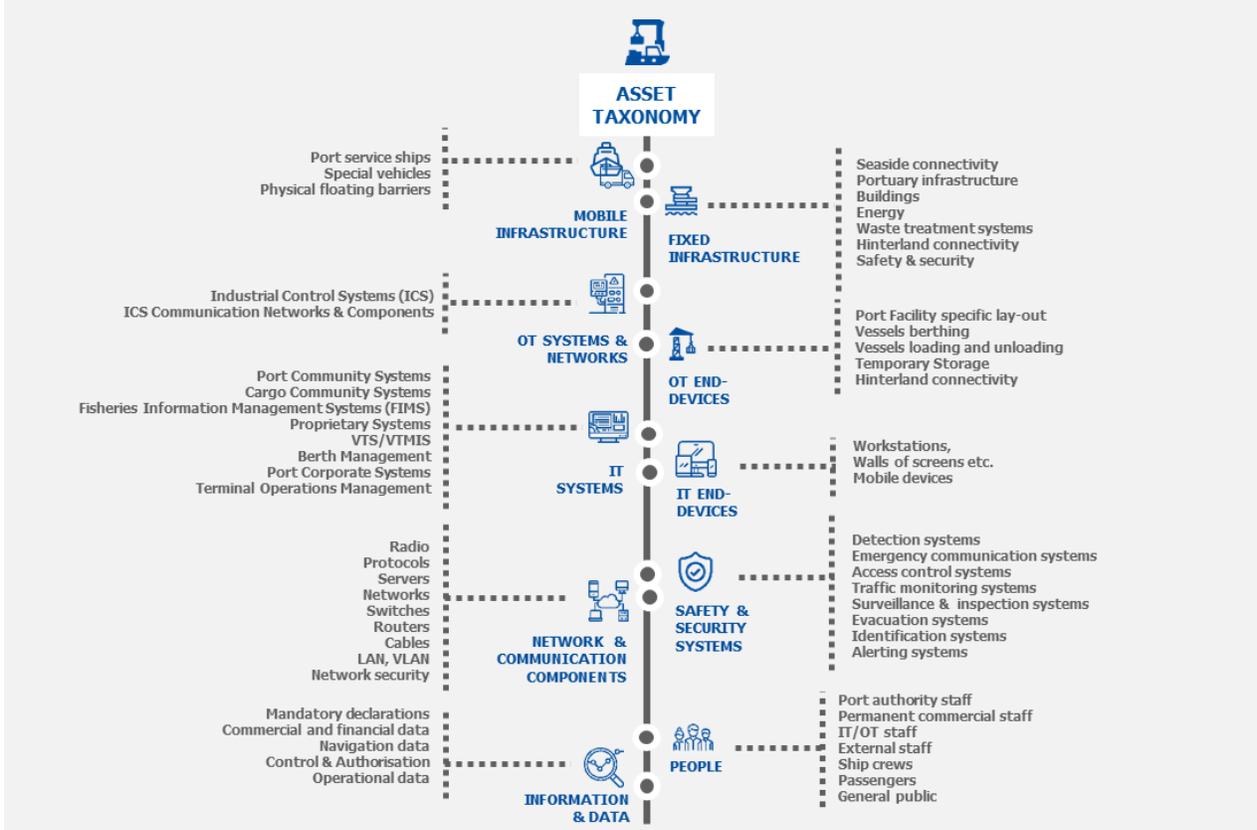


Figure 13: The ENISA taxonomy for critical maritime assets (Source: [ENISA 2019])

Concerning **autonomous ships**, their critical assets may include systems like those described above, as well as additional systems. The operational ecosystem of autonomous ships is depicted in Figure 14. The International Maritime Organization (IMO) formally refers to the autonomous ship as *Maritime Autonomous*

*Surface Ship* (MASS). The Norwegian Forum for Autonomous Ships (NFAS) has provided a description for the context of MASS shown in Figure 14 [AGK 2019].

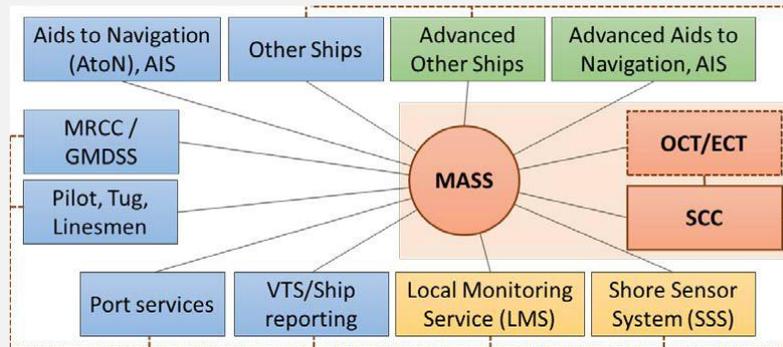


Figure 14: Context diagram for autonomous ship operation (Source: [RN 2017])

The MASS components are briefly described below [AGK 2019]:

- **Shore Control Centre (SCC):** A controlling entity, also called the remote-control centre (RCC). It monitors the status of an autonomous ship and partially controls it according to the implemented autonomy level. Because of regulation [RT 2014], a certain manning requirement is expected.
- **ECT/OCT:** In case of emergency (e.g. loss of communication with the ship), an external emergency control team (ECT) may enter the ship to provide the necessary help. In an autonomous ship that is only periodically unmanned, in certain voyage phases, an on-board control team (OCT) may take control of the ship.
- **Shore Sensor System (SSS):** Sensors are expected to be deployed on the shore side to aid certain functions and operations, such as automatic docking.
- **VTS/LMS/RIS:** A group of marine traffic services, such as vessel traffic services (VTS), local monitoring services (LMS), and river information services (RIS), are required to be provisioned in order to facilitate navigation.
- **Aids to Navigation (AtoN):** Navigation depends on several systems for real-time information related to weather, positioning, etc. These include the global navigation satellite system (GNSS) for positioning, automatic identification system (AIS) for traffic coordination, in addition to radar, LIDAR (Light Detection And Ranging) and other systems used for situational awareness.
- **MRCC/GMDSS:** The maritime rescue coordination centre (MRCC) and global maritime distress and safety system (GMDSS) are both radio services for emergencies. Depending on the size of the ship and the operational area, some autonomous ships are expected to follow certain regulations to answer distress or emergency signals, or may also benefit from such services.
- **Other Ships:** This involves the other ships operating around an autonomous ship. All ships, including autonomous ones, are expected to communicate for safety reasons using common communication systems such as VHF, VHF Data Exchange System (VDES) or others.
- **Port Services:** Services related to logistics and supply are expected to be arranged, such as automatic mooring and electric charging.
- **Service vessels:** Assistance from various service vessels, such as pilots, tugs or others, should be arranged.

### 7.3.2 What is expected to go wrong?

In 2018, several ports reported cyber security incidents, e.g. Maersk ransomware attack disrupting operations in 76 port terminals globally, the Port of Barcelona US Ports (Long Beach, San Diego), Austal, Royal Navy of Oman. ENISA [ENISA 2019] has provided the maritime cyber threat landscape, depicted in Figure 15:

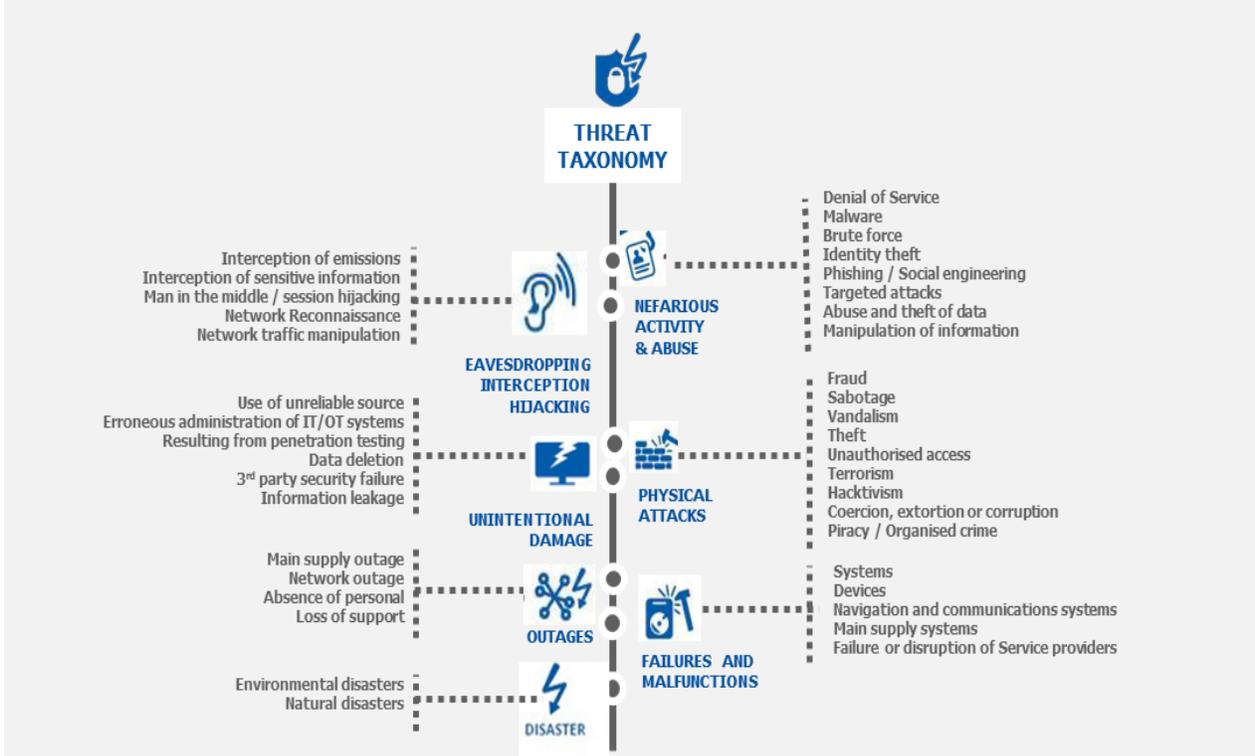


Figure 15: The ENISA threat taxonomy for the maritime transport sector (Source: [ENISA 2019])

Common maritime threats reported are:

- GPS spoofing
- Unauthorized access to on-board mobile devices
- Manipulation of bill of lading
- Signal jamming, monitoring
- Targeted access to automated terminal infrastructures (e.g. electronic gates, RFIDs in containers, cameras, surveillance systems)
- Spear phishing, DoS
- Supply chain attacks
- IoT attacks

New emerging technologies will provide new threats to the maritime ecosystem e.g.:

- International **Supply chains**, **AI** and **5G technologies** may be utilized by malicious entities as attack enablers against interconnected vessels, by exploiting non-obvious interactions among such systems.

- The on-board connected IT systems (e.g. cargo management, bridge systems, passengers servicing, communication systems, etc.) increasingly tend to be provided by international suppliers **with non-EU security certifications**, who are more vulnerable to attacks.
- The vessels are controlled by their inland shipping company, but operated by their on-board technical departments who may lack the necessary cyber skills. Thus, a **lack of cyber-skills** will be an upcoming threat.

### 7.3.3 What is the worst thing that can happen?

For the maritime case an implementation of the impact as described in the methodology section (2.1) is applied for the agent profile instances and the corresponding incidents presented in the previous chapter. To evaluate the impact on each asset the worst-case impact on confidentiality, integrity and availability are considered.

The worst types of impact provided by NIST and identified in the maritime case are the following:

- Harm to Operations
  - Inability to perform current missions/business functions.
  - Inability, or limited ability, to perform missions/business functions in the future.
  - Harms (e.g. financial costs, sanctions) due to noncompliance.
- Harm to Assets
  - Damage to or loss of physical facilities
  - Damage to or loss of information systems or networks.
  - Damage to or loss of information technology or equipment.
- Harm to Individuals
  - Injury or loss of life.
  - Physical or psychological mistreatment.
  - Identity theft.
  - Loss of personally identifiable information.
- Harm to the Environment

## 7.4 Who are the attackers?

Because of the globalization of the sector, all categories of attackers are possible. In this section the agent profiles described in the methodology (section 2.1) are further adjusted to fit the sector-specific requirements of the maritime transport case. In this regard, possible instances of the maritime threat agent profiles reflected by prominent maritime security incidents are listed.

### 7.4.1 Maritime Threat Agents

#### 7.4.1.1 Agent: Activists

**Instance:** Hacktivists

**Incident:** A hacktivist group calling itself by the evocative name “Cutting Sword of Justice” claimed responsibility for the Saudi Aramco hack, in posts to Pastebin. The group said the hack was to avenge the “atrocities taking place in Syria, Bahrain, Yemen, Lebanon [and] Egypt” and seemed to suggest that Shamoon was the malware used in the attack.

#### 7.4.1.2 Agent: Competitor

**Instance:** Ruthless Competitor

**Incident:** A French submarine maker DCNS was hit by a data leak in 2016. Some sources maintain that the attack came from rival companies attempting to assert dominance in the market and undermine their competitors.

#### 7.4.1.3 Agent: Corrupt Government Official

**Instance:** Corrupt Port Official/Third Party

**Incident:** In a case presented in Singapore, Public Prosecutor vs. Syed Mostofa Romel, bribery charges were filed against Syed Mostofa Romel, an associate consultant in the marine surveying business of PacMarine Services Pte Ltd.

#### 7.4.1.4 Agent: Cyber Vandal

**Instance:** Hacker

**Incident:** Maersk has revealed the financial impact caused by the NotPetya ransomware attack. According to a statement issued by the company, the total cost of dealing with the outbreak will be somewhere in the \$200 to \$300 million range.

#### 7.4.1.5 Agent: Data Miner/Thief

**Instance:** Ransom Holder

**Incident:** British shipping services firm Clarkson Plc revealed details of a cyber security incident that took place in 2017. An unauthorized third party gained access to the company's computer systems in the UK, copied data, and demanded a ransom for its return.

#### 7.4.1.6 Agent: Employee, Disgruntled

**Instance:** Stressed Employee

**Incident:** There is a report of malware infecting offshore rigs in the Gulf of Mexico. This incident was caused by offshore workers, who put in long and gruelling 14-day shifts at sea. During the nights, they disrupted computer networks on rigs in the Gulf of Mexico after unintentionally downloading malware in their spare time. Those employees inadvertently exposed vulnerabilities in their network security that posed serious long-term threats.

#### 7.4.1.7 Agent: Government Spy

**Instance:** Foreign Government Surveillance

**Incident:** Between June 22-24 2017, a number of ships in the Black Sea reported anomalies in their GPS-derived position, and found themselves apparently located at an airport. Some sources indicate that the incident was the result of an attempt at undetected drone surveillance of the area by foreign governments.

#### 7.4.1.8 Agent: Government Cyberwarrior

**Instance:** Foreign Government Sabotage

**Incident: Gulf of Oman.** On 12 May 2019, four commercial ships were damaged off the Fujairah coast in the Gulf of Oman. The United States accused the Iran Revolutionary Guard Corps (IRGC) of being "directly responsible" for the attacks.

#### 7.4.1.9 Agent: Internal Spy

**Instance:** Whistleblower

**Incident:** The British engineer who recorded the illegal dumping of oily waste from the Caribbean Princess will receive \$1 million of the \$40 million fine paid by Princess Cruise Lines on Wednesday. Princess was sentenced to pay a \$40 million penalty, the largest recorded amount for crimes involving deliberate vessel pollution. The sentence was imposed by US District Judge Patricia A. Seitz in Miami.

**7.4.1.10 Agent: Sensationalist/Irrational Individual****Instance:** Deranged Individual

**Incident:** Gary McKinnon, a Scottish systems administrator and hacker, obtained administrator privileges, installed hacking tools and deleted system logs on 14 computers in Groton, Connecticut, and six at other US Navy sites, including Pearl Harbor. Security experts remained unimpressed, however, by his technical skills. He went on to attack multiple authorities.

**7.4.1.11 Agent: Terrorist****Instance:** Terrorist

**Incident:** In February 2017, hackers reportedly took control of the navigation systems of a German-owned 8250-ton container vessel en route from Cyprus to Djibouti for 10 hours. “Suddenly the captain could not manoeuvre,” an industry source who did not wish to be identified told Fairplay sister title Safety At Sea (SAS). “The IT system of the vessel was completely hacked.” There are indications that the hackers were from terrorist organizations.

**7.4.1.12 Agent: Mobster****Instance:** Pirate

**Incident:** In Somalia, tech-savvy pirates once breached the servers of a global shipping company to locate the exact vessel and cargo containers they wanted to plunder. Later, a malicious web shell was found that had been uploaded onto the server.

**7.4.1.13 Agent: Mobster****Instance:** Drug Trafficker

**Incident:** The attack on the port of Antwerp is thought to have taken place over a two-year period from June 2011. According to publicly available information, a Dutch-based trafficking group hid cocaine and heroin among legitimate cargoes, shipped in containers from South America. The organized crime group allegedly used hackers based in Belgium to infiltrate computer networks in at least two companies operating in the port of Antwerp.

**7.4.1.14 Agent: Mobster****Instance:** Weapon trafficker

**Incident:** In September 2017, a local maritime police force in Puntland seized a boat that had a large cache of machine guns, small arms, ammunition, and anti-aircraft guns. The crew of the boat escaped, but it is believed they were bringing these weapons from Yemeni waters. Eventually the weapons could have made their way into the hands of al-Shabaab, the Islamic State, or any of the various clan-based militias.

**7.4.1.15 Agent: Mobster****Instance:** Human Trafficker

**Incident:** In 2017 Thirteen African migrants suffocated inside a shipping container while being transported over four days between two Libyan towns.

## 7.5 Major incidents in this vertical

The incremental use of digital technology in the maritime transport CIs and their interdependent nature have attracted the attention of threat agents who are continuously improving their cyber skills, implementing progressively more complex and sophisticated attacks. The most important categories of threat agents have been described in section 7.4.1. According to Hellenic Shipping News,<sup>309</sup> from 2017-2020 there was a tremendous increase of 900% in cyberattacks on maritime transport OT systems, with an unprecedented increase in the volume of reported incidents by each year end. In fact, in 2018 there were more than 500 major cybersecurity breaches, excluding several more unreported. Two distinct types of cyberattack are underlined in the maritime transport environment: untargeted attacks (looking for potential cyber weak spots, either in multiple maritime transport companies or on ships), and targeted attacks, which target a specific company or ship and can be harder to tackle. Well-known maritime security (cyber and/or physical) incidents are presented in section 7.4.1 as examples of each threat agent category. In addition, other major incidents that have affected the Maritime Transport vertical are summarised below.

In recent years, alarming new coordinated scenarios are causing mass atrocities and severe repercussions in Maritime Transport. A series of ransomware attacks have been witnessed within the maritime transport sector over the past years.

- Indicatively, during May 2017, Lyttelton Port, the largest port in the south island of New Zealand experienced a temporary eight-hour shutdown to secure its IT system after a WannaCry security threat from a cyber group.<sup>310</sup>
- In June 2017, the NotPetya ransomware attack hit the industry giant Maersk, impacting operations in terminals of 4 countries and causing delays and disruption that lasted weeks.<sup>311</sup>
- During the same period, operations at one of the three terminals of Jawaharlal Nehru Port Trust (JNPT), India's largest container port in Mumbai, came to a standstill after a global ransomware attack directed at Russia's biggest oil company and multinational EU companies.
- In 2017, at least 20 ships in the Black Sea near Novorossiysk stated that their navigation systems were showing a position that was 32 km away from their actual positions as a result of GNSS spoofing [MBWRN 2021].
- In July 2018, COSCO confirmed that it was hit by a ransomware attack that disabled emails and telephone systems and shut down connections to other regions.<sup>312</sup>

<sup>309</sup> Hellenic Shipping News, <https://www.hellenicshippingnews.com/maritime-cyber-attacks-increase-by-900-in-three-years/>

<sup>310</sup> Maddison Northcott, <https://www.stuff.co.nz/the-press/business/92613020/urgent-outage-at-lyttelton-port-after-wannacry-cyber-attack>

<sup>311</sup> Hindustan Times, Cyberattack: Ransomware hits Jawaharlal Nehru port operations in Mumbai, <https://www.hindustantimes.com/india-news/cyber-attack-malware-hits-jawaharlal-nehru-port-operations-in-mumbai/story-xGtbHwvZI4bX5RgJCUBN3L.html>

<sup>312</sup> Offshore Energy, <https://www.offshore-energy.biz/cosco-shipping-lines-falls-victim-to-cyber-attack/>

- A mysterious set of “sabotage attacks” occurred in May 2019, when 4 tankers experienced a cyberattack at Fujairah anchorage, United Arab Emirates, linked with a drone performing underwater attacks with high grade explosives.<sup>313</sup>
- During 2019, a tanker near the port of Naantali in Finland became infected by ransomware in its administration server. Remote Desktop Protocol (RDP), a USB device or an email attachment are considered possible attack resources. After four months, the same vessel was infected again, close to the same port [MBWRN 2021].
- The increasing use of online services in towage vessels has raised cyber threats in such infrastructures. During 2020, a US tugboat was hit by cyberattackers.<sup>314</sup>
- In July 2020, the Mediterranean Shipping Company (MSC) was infected by an unnamed malware strain. The incident was limited to MSC’s headquarters in Geneva and affected the availability of some of the company’s digital tools on its website for a few days during the Easter holiday.
- In October, 2020, the IMO maritime standardisation body was hit by a cyberattack on their IT systems, while the world’s third largest container line, CMA CGM, faced the Ragnar Locker ransomware attack on its Chinese branches (Shanghai, Shenzhen, and Guangzhou). The latter attack involved malware that put the company’s e-commerce systems (i.e. its worldwide shipping container booking system) offline and produced a suspected data breach.<sup>315</sup>
- Another ransomware attack occurred in the Port of Kennewick in 2020. The hackers demanded a ransom of 200,000 USD, which was not paid, leaving systems unavailable for several days [MBWRN 2021].<sup>316</sup>
- In June 2021, South Korea’s national flagship carrier, HMM, experienced a cyberattack that affected the company’s email server.<sup>317</sup>
- In November 2021, cyberattackers committed multiple attacks impacting Greek shipping firms. The malware was spread via the systems of Danaos Management Consultants, a well-known IT consulting firm.<sup>318</sup>

## 7.6 Research Challenges

The complicated dual physical/cyber nature of the maritime environment raises a set of open issues concerning the effective and efficient handling of their security and safety issues. In this context, we have identified a set of research challenges and issues, regarding the distributed and interconnected nature of complex, interrelated maritime components, network and operating environments that need to be investigated within and beyond the current project. The challenges for this case are indexed to their corresponding JRC taxonomy sectors and presented along with a description for this vertical.

<sup>313</sup> World Maritime News, <https://www.offshore-energy.biz/uae-state-actor-likely-behind-sophisticated-fujairah-attacks/>

<sup>314</sup> I.G. Macola, Ship Technology, US Tugboat cyber-attack: the experts respond, <https://www.ship-technology.com/features/cyber-attacks-in-the-maritime-sector-the-experts-respond/>

<sup>315</sup> ZDNet, <https://www.zdnet.com/article/all-four-of-the-worlds-largest-shipping-companies-have-now-been-hit-by-cyber-attacks/>

<sup>316</sup> Maritime Executive: Ransomware Cripples IT Systems of Inland Port in Washington State, <https://www.maritime-executive.com/article/ransomware-attack-cripples-systems-of-inland-port-in-washington-state>, last accessed 2021/04/25

<sup>317</sup> Offshore Energy, HMM hit by cyber attack, <https://www.offshore-energy.biz/hmm-hit-by-cyber-attack/>

<sup>318</sup> The Maritime Executive. Cyberattack Hits Multiple Greek Shipping Firms, <https://www.maritime-executive.com/article/cyberattack-hits-multiple-greek-shipping-firms>

## 7.6.1 State of the Art

The first version of the “Research and Development Roadmap” [Markatos 2020] included an initial investigation of what is at stake in the area of maritime transport as regards cybersecurity. An analysis of the security requirements of the domain’s critical infrastructures, who are the attackers and their profile, was conducted, and a series of research security challenges and issues related to the maritime transport were discussed. These included the early identification and assessment of risk requirements, the detection of threats and attack paths for critical maritime systems, the need to focus on security hardening for maritime transport systems, the importance of maintaining the resilience of critical maritime systems, and the need to preserve maritime system communication security and to keep up the security in autonomous ships.

In the second version of the “Research and Development Roadmap” [Markatos 2021], a state-of-the-art analysis was presented to capture the existing research in maritime transport cybersecurity, with respect to the research challenges identified. In this section we will update the state-of-the-art analysis, to include additional research efforts in the field that took place during the last year.

In this section, a desktop research analysis is presented to better capture the state of the art in maritime transport with respect to these research challenges.

### 7.6.1.1 Legal and regulatory background

A variety of legal frameworks, general international and European standards, guidelines and best practices in the field of information security and risk management for critical infrastructures have been applied to organisations in the maritime transport sector.

Regarding cybersecurity, in December 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy established a new EU Cybersecurity Strategy [EC 2020A] that aims to build resilience to cyber threats and ensure citizens and businesses benefit from trustworthy digital technologies.

Delegated regulations concerning network and information security, and the protection of critical information infrastructure, are the EU NIS Directive [NIS DIRECTIVE 2016] and the legislative proposal of NIS 2.0 [NIS 2 DIRECTIVE 2020], which contains measures for improving cybersecurity infrastructure and particularly the resilience and incident response capabilities of public and private competent authorities. The NIST Framework provides guidance to improve critical infrastructure cybersecurity [NIST 2018]. The EU regulation No 881/2019 [EU 881/19, 2019] establishes cybersecurity certification of products, processes and services. NIST SP 800-82 provides guidance on the security of industrial control systems (ICS) [NIST 2015B]. Generic frameworks and good practices for risk management are considered by the NIST SP 800-30 risk assessment publication [NIST 2012], the Risk Management Framework on Information Systems and Organizations [NIST 2018B], the NIST SP 800-55 Performance Measurement Guide for Information Security [NIST 2020] and the NIST Supply Chain Risk Management practices in [NIST 2015] [NIST 2019].

Some major ISO standards pertaining to this area are the ISO 31000:2018 Risk Management generic standard [ISO31000 2018] in terms of finance, engineering and security the ISO/IEC27005:2018 Risk Management standard [ISO/IEC27005 2018] specifically for information security and other standards of

the ISO27k family for Information Security Management Systems (ISMS), such as [ISO/IEC27000 2018; ISO/IEC27001 2013; ISO/IEC27002 2013]. In the [ISO/IEC31010 2019] standard well-known risk management and risk assessment techniques are highlighted, including the Delphi method [CSS, 1999], Event Tree analysis [CRS 1998], Fault Tree Analysis [Ericson, 1999], Structured What If Technique (SWIFT), Markov Analysis [Gagniac 2017] and Monte Carlo Simulation [Hastings 1970].

Concerning the manner of assessment in terms of targeting cybersecurity certification, ENISA has published a methodology for sectoral cybersecurity assessment [ENISA 2021A], providing guidance on ICT security for sectoral multi-stakeholder systems and drafting sectoral cybersecurity certification schemes that can be utilized for the maritime transport sector, as they implement a variety of ICT services.

A series of annual reports have been published by ENISA within the last 9 years: the “ENISA Threat Landscape” (ETL) reports, which refer to the general cybersecurity threat landscape of the reported period, highlighting prime threats, major trends towards threats, threat actors and attack techniques, and respective mitigation measures. In its 9<sup>th</sup> edition in 2021 [ENISA 2021C], the report underlines cybercrime threats to the Transport Industry that have already affected widely known maritime shipping and logistics enterprises.

The ENISA report on communication network dependencies for ICS/SCADA Systems [ENISA 2017A] provides insight into the communication network interdependencies of current industrial infrastructures and environments against potential attacks, with a view to identifying best practices and security measures.

Widely known technical standards and specifications for IT/network security and Industrial Control Systems (ICSs) are indicatively the ISO/IEC 27033 standard on information security and network security technology, which consists of 6 parts<sup>319</sup>, the EVS-EN ISO/IEC 15408-3:2020<sup>320</sup> and EVS-EN-ISO/IEC 18045:2020<sup>321</sup> standards related to the assurance requirements of the IT security evaluation criteria and methodology accordingly the EN ISO/IEC 19790:2020<sup>322</sup> standard including cryptographic modules and the EN ISO 29134:2020<sup>323</sup> standard on privacy impact assessment. In this line, European Telecommunications Standard Institute (ETSI) sets protocols on advanced networking and risk analysis (ETSI TR187002 2011<sup>324</sup>; TVRA ETSI TS 102 165-1 V5.2.3 2017<sup>325</sup>).

A large number of older, well-known, traditional risk management methods and risk assessment tools can be found in the ENISA’s inventory of risk management and RA methods [ENISA 2020]. These include the EBIOS method used by ANSSI [ANSSI EBIOS 2020], the OCTAVE method [Tucker 2020], based on a Bayesian approach using UML, the Magerit open methodology for risk analysis and risk management, and the Mehari method for harmonized risk analysis [CC 2018]. In addition, BowTie [IP Bank 2015] is a primarily qualitative risk analysis method that is in wide use, while CORAS [LSS 2010] is a method that promotes the use of model-driven security risk analysis. Given the complexity and cross-sectoral nature of

---

<sup>319</sup> <https://www.iso27001security.com/html/27033.html>

<sup>320</sup> <https://www.evs.ee/en/evs-en-iso-iec-15408-3-2020>

<sup>321</sup> <https://www.evs.ee/en/evs-en-iso-iec-18045-2020>

<sup>322</sup> [https://www.cenelec.eu/dyn/www/f?p=104:110:609928853661101:::FSP\\_ORG\\_ID,FSP\\_PROJECT,FSP\\_LANG\\_ID:2307986,69303,25](https://www.cenelec.eu/dyn/www/f?p=104:110:609928853661101:::FSP_ORG_ID,FSP_PROJECT,FSP_LANG_ID:2307986,69303,25)

<sup>323</sup> [https://www.cenelec.eu/dyn/www/f?p=104:110:1727884474979701:::FSP\\_ORG\\_ID,FSP\\_PROJECT,FSP\\_LANG\\_ID:2307986,69257,25](https://www.cenelec.eu/dyn/www/f?p=104:110:1727884474979701:::FSP_ORG_ID,FSP_PROJECT,FSP_LANG_ID:2307986,69257,25)

<sup>324</sup> [https://www.etsi.org/deliver/etsi\\_tr/187000\\_187099/187002/03.01.01\\_60/tr\\_187002v030101p.pdf](https://www.etsi.org/deliver/etsi_tr/187000_187099/187002/03.01.01_60/tr_187002v030101p.pdf)

<sup>325</sup> [https://www.etsi.org/deliver/etsi\\_ts/102100\\_102199/10216501/05.02.03\\_60/ts\\_10216501v050203p.pdf](https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/05.02.03_60/ts_10216501v050203p.pdf)

maritime transport, maritime critical infrastructures are vulnerable to various threats and cannot be addressed by traditional risk assessment methodologies [AWW 2017] [Boyson 2014].

#### 7.6.1.1.1 Security law, standards and best practices in the maritime transport sector

Sector-specific laws, legal frameworks and standards for maritime transport are provided for both the physical and the cyber planes. The Safety of Life at Sea (SOLAS) Convention (1974/1988) is a maritime treaty on minimum security arrangements for ships, ports and government agencies [IMO 2003] (e.g. MSC.: 286(86), 256(84), 46(66), 291(87), 216(82), 282(86), 291(87), 290(87)). The International Ship and Port Facility Security (ISPS) Code [IMO 2004] (an amendment to the SOLAS convention) and the respective EU regulation which ensures it [EC725/2004] define a set of measures to expand security for port facilities and ships. The International Convention for the Prevention of Pollution from Ships “MARPOL 73/78” from the IMO is the main international convention for sea protection, specifically for the prevention of pollution of the marine environment by ships, either operational or accidental. The EU regulation on maritime safety mainly engages EU Directive 2002/84/EC, which reflects the prevention of pollution from ships and the effects of shipboard living and working conditions, while EU Regulation (EC) No 1406/2002 sets up the European Maritime Safety Agency [EMSA 2020A] to address maritime safety and maritime security issues (including pollution prevention) in the European Union. EU Directive 2002/59/EC, the 2010 “EU maritime information and exchange system”, concerns a vessel traffic monitoring and information exchange system and addresses the exchange and sharing of additional information to facilitate maritime traffic and transport in an efficient manner.

The EU Maritime Security Strategy (EUMSS) EU JOIN(2014) 9 [EC 2014] applies a security strategy for an open and secure global maritime domain in order to facilitate a cross-sectoral approach to maritime security. During 2020, the European Commission provided an action plan that implements the EUMSS in the following 5 key areas: (i) international cooperation, (ii) maritime surveillance, (iii) capability development - research and innovation, (iv) risk management, education and (v) training [EC 2020B] (further discussed in Section 7.6.8.2.)

During 2017, the Maritime Safety Committee adopted the Resolution MSC.428(98), “Maritime Cyber Risk Management in Safety Management Systems” [IMO 2017C]. The Resolution highlights that cyber risk management should be considered in existing maritime safety management systems with regard to the objectives and requirements of the International Safety Management (ISM) Code.<sup>326,327</sup> In this context, identifying, analysing, assessing and communicating cyber-related risks, as well as conducting mitigation measures, is recommended. As such, IMO invited countries to “appropriately address” the underlined pre-existing requirements no later than January 1, 2021, and urged ship owners and maritime transport operators to comply with Resolution MSC.428(98). In this regard, IMO encourages Flag States not to issue compliance documents to vessels if cyber risks are not adequately addressed in the corresponding safety management system. For this purpose, the IMO Convention on Facilitation of International Maritime Traffic (FAL) has set guidelines for maritime cyber risk management in MSC-FAL.1/Circ.3 [IMO 2017B],

<sup>326</sup> <https://imo-2021.com/>

<sup>327</sup> SAFETY4SEA: Guidelines on maritime cyber risk management, <https://safety4sea.com/guidelines-on-maritime-cyber-risk-management/>

indicating how to conduct an assessment of the cyber risks to be compliant with the Resolution [IMO 2017C]. In addition, BIMCO has published guidelines on Cybersecurity On Board Ships [BIMCO 2021A] and has provided additional guidance in the publication of a “Cyber Security Workbook for On Board Ship Use” [BIMCO 2021B], including comprehensive step-by-step checklists to help ship owners, ship managers and ports deal with the practical, day-to-day management of on-board cyber security and be compliant with the IMO Resolution requirements. Such guidelines are also available from other associations: i.e. the Digital Container Shipping Association’s (DCSA) “DCSA Implementation Guide for Cyber Security on Vessels v1.0”, an analysis of version 3 of these guidelines and the NIST framework. While the target audience for DCSA’s guidelines is the container industry, it may also be valuable for other segments.

A growing number of initiatives regarding vulnerabilities of vessel information systems that render ships subject to cyberattacks have been identified within the last six years [DNV GL 2016;2020; ABS 2018]. In relation to maritime cybersecurity, the International Association of Classification Societies (IACS) has provided the IACS Rec. 2020/Corr.1 2020 recommendations on providing technical requirements to maritime stakeholders. Implementation of these requirements would result in cyber resilient ships, whose resilience can be maintained over their service life [IACS 2020]. During 2021, The Inmarsat Research Programme has published good practices for the design, deployment and ongoing operational management of shipboard ICT systems [INMARSAT 2021]. It provides guidance on how to maximise uptime and minimise cyber vulnerabilities of on-board networks and automated systems.

Maritime security topics are addressed by the ISO 28005-1:2013 standard on security management systems for the supply chain, which defines technical specifications that facilitate a sufficient exchange of electronic information between vessels and shore for coastal transit or port calls aiming to support the IMO FAL Convention and other international specifications. ISO 28007-1:2015 on Ships and marine technology gives guidelines for Private Maritime Security Companies (PMSC), addressing privately contracted armed security personnel (PCASP) on board ships. The ISO 20858:2007 standard [ISO20858 2007] establishes a framework to assist marine port facilities in specifying the competence of personnel to conduct a marine port facility security assessment and develop a security plan as required by the ISPS Code. Other statutory initiatives in maritime physical security are the Container Security Initiative (CSI), the Customs-Trade Partnership against Terrorism (C-TPAT), and the 24-hour advance vessel manifest rule [UNCTAD 2006].

With respect to maritime cybersecurity, ENISA has published a report on “Cyber Security Aspects in the Maritime Sector” [CMB+ 2011]. In addition, regarding port cybersecurity, ENISA has released good practices and guidelines to port stakeholders [ENISA 2019] and at the end of 2020 published an updated report on maritime cybersecurity regarding cyber risk management of ports [ENISA 2020E]. As a result, the legal background in maritime security is mainly focused on physical security. Recently, there have been considerable efforts to address the legal aspects of maritime cybersecurity. However, they are still considered to be new areas for investigation.

#### **7.6.1.2 Risk assessment in the maritime transport sector**

To better illustrate the presentation of state-of-the-art risk assessment methods and tools in maritime transport, the noteworthy existing literature is categorized into the two following topics: traditional maritime risk assessment methods and cybersecurity risk assessment on autonomous/semi-autonomous ships, which are described in the following paragraphs.

#### 7.6.1.2.1 Traditional maritime risk assessment methods

Traditional methods for maritime security management include the Maritime Security Risk Analysis Model (MSRAM), along with its extended version MSRAM-PLUS/FORETELL, which is ISPS compliant and addresses only physical security; the Maritime Integrated Surveillance Awareness method, also known as the MARISA method, geared towards the safe navigation of ships during their presence in port; the CMA, for detecting abnormal behaviour of ships and capturing respective threats; and the SafeSeaNet, which collects maritime information from national authorities and national methodologies (i.e. Estonia, Jordan, Russia), focusing on the safety of ports. As yet, research work on the identification of asset vulnerabilities, cyber threats and risks specifically for the maritime transport domain is limited. However, maritime cyber risk assessment methods have recently begun to appear.

#### 7.6.1.2.2 Other risk assessment methods and cybersecurity approaches for maritime transport Critical Infrastructures protection

Most critical maritime transport services incorporate both physical processes (e.g. stevedoring, port plant power supply) and cyber operations (remote monitoring, historical data storage on power supply operations) which are regulated through complex, multimodal cyber-physical systems, such as the Industrial Control Systems (ICS), including the Supervisory Control and Data Acquisition (SCADA) systems and the Distributed Control Systems (DCS) [KPMP 2018].

A potential cyberattack on a cyber-physical system could have a tremendous impact on the maritime transport sector, including damage to infrastructure, environmental harm, or even the loss of human life. For example, an LNG fuel remote control system compromise could allow adversaries to take control of LNG tankers and turn them into floating bombs. In this vein, since the composite SCADA-based infrastructures engage security specificities and network particularities, a thorough study of their vulnerabilities, threats and risk, and a deep analysis to understand parameters such as the causes of vulnerabilities are strongly required. Most SCADA and ICTs began as proprietary, standalone systems that were separated from the rest of the world and isolated from most external threats, whereas more recent SCADA systems have moved to more interoperability and open standards for cost efficiency and integration into management IT systems. For instance, communication is now common over Ethernet TCP-IP, including more standardized control protocols and applications.

Open standards for SCADA systems are sources for adversaries to gain knowledge regarding the SCADA network topology [ILW 2006]. [PR 2005] proposes an assessment approach for SCADA system, including reconnaissance procedures to gather information on the target system, perform vulnerability scanning within the SCADA network, and meet the targets of evaluation (TOEs) identified in the assessment plan. In addition, they a list of open source and commercial tools for assessing SCADA systems has been presented (e.g. NMAP, NESSUS, STAT SCANNER, ETHEREAL, ETTERCAP, DEBUGGERS, FUZZERS, etc.). Quantifying vulnerability methods for critical infrastructures are introduced by [CDV 2013]. SCADA systems are subject to external attacks and IT-based vulnerabilities, as presented in [KPMP 2018]. Deficiencies in security controls can occur as a result of the lack of cryptography policies used in SCADA networks [ILW 2006] or unskilled, naive employees revealing passwords to colleagues, ignoring the potential risk [DUS+ 2012]. A cyber terrorism SCADA Risk framework is demonstrated in [BW 2009]. Considerable risk assessment methods for SCADA systems have been introduced [TEA 2019; CBB 2016;

CAL+ 2016] to meet a broader scope than risk assessment and also describe modules for attack detection and automated response to an attack. [KKN+ 2020] presents a regression analysis and [TML 2010] engages real-time monitoring, anomaly detection, impact analysis and mitigation strategies for SCADA infrastructures. [MSR 2019] presents a novel method for security risk assessment in SCADA networks, dividing it into three phases: the objective phase, the subjective phase and the final assessment phase, utilizing fuzzy logic in all phases and an analytical hierarchy process (AHP) in the subjective phase. A cyberattack detection subsystem and a risk assessment framework is illustrated in [FMP+ 2018]. Yang et al [YCG 2019] develop a SCADA security assessment for oil and GAS SCADA systems, utilizing the fuzzy Mamdani reasoning to evaluate factor neurons.

The Cyber/Physical Security Management System (CYSM) approach [PPK 2015] is based on collaboration among maritime transport stakeholders and addresses the security and safety requirements of commercial ports' critical information infrastructures (CII). The MEDUSA<sup>328</sup> risk assessment method [PKP 2016] undertakes Multi-ordEr Dependency approaches for managing cascading effects in a port's global sUpply chain and their integration in riSk Assessment frameworks, which aim to fine tune the organisation's security policies according to their business role, together with their inherent dependencies. The MITIGATE<sup>329</sup> methodology [PP 2018; KPMP 2018] is a dynamic risk assessment methodology for the maritime supply chain, which addresses the specificities and particularities of ICT infrastructures, mainly of ports, and evaluates their evolving risk landscape by identifying interdependencies between assets and their associated threats, along with the cascading effects.

Papastergiou et al [PKP 2021] present risk assessment results from realistic use-cases, to validate the MITIGATE methodology in several scenarios of maritime supply chains.

In relation to IMO 2021 compliance, which raises the conformance of maritime transport operators with the cybersecurity requirements of IMO Resolution MSC.428(98) [IMO 2017C] "Cydome" is a cybersecurity suite for the maritime transport industry, providing on-the-fly visibility on vessel fleet to protect vessels from inside and outside attacks.<sup>330</sup>

### 7.6.1.2.3 Cybersecurity risk assessment on autonomous/semi-autonomous ships

Currently, the maritime transport sector is targeted at the development of next-generation ships, such as smart ships, and semi-autonomous or autonomous ships [BTB+ 2020; AUTOSHIP 2019; MH 2019; Daffey 2018; MUNIN 2016; AAWA 2016]. The deployment of maritime autonomous surface ships (MASS) is an emerging technological trend towards the potential to advance vessels' safety and efficiency and optimize their performance [RN 2017]. In this area, the reliability, availability, maintainability and safety of autonomous ships must be ensured, and thus the performance of risk assessment is necessary to confirm the maintenance of the ships' safety [URS+ 2020]. Several research projects on risk assessment for autonomous and semi-autonomous ships have been identified and are further analysed in section 7.6.1.5.

---

<sup>328</sup> MEDUSA stands for Multi-ordEr Dependency approaches for managing cascading effects in port's global sUpply chain and their integration in riSk Assessment frameworks

<sup>329</sup> MITIGATE stands for Multidimensional, IntegraTed, riSk assessment framework and dynamic, collaborative risk manaGement tools for critical information infrAstrucTrurEs

<sup>330</sup> CYDOME, <https://cydome.io/>

The literature reviews place strong emphasis on physical security, a lack of maritime cybersecurity awareness with respect to highlight information on attacks and vulnerabilities, and a lack of cybersecurity training on the part of port and logistics personnel and maritime transport stakeholders [DGR 2015].

On this basis, there is a compelling need to develop security solutions that raise maritime cybersecurity awareness.

### 7.6.1.3 Security hardening for critical (maritime) systems

Security hardening is a common approach for addressing security problems without actually *correcting* the underlying error. Hardening essentially assumes that fixing the error in the first place is a difficult task, or sometimes impossible. What remains, as a possible solution, is to make a system functional, including potential errors. The approach for this is to *harden* the system, which reflects a state where system errors have significantly less severe consequences compared to the non-hardened system. For instance, memory hardening is applied commonly to address memory-corruption vulnerabilities. Assuming there is a system with a memory-corruption vulnerability, then typically, this system is likely to be compromised (i.e. controlled by an attacker), while the hardened version of it will at most produce a crash (less severe than a system compromise).

Hardening techniques are an attractive approach in domains where it is hard to analyse and correct software errors. Typically, this includes systems, or ecosystems, that are based on non-standard devices, embedded systems, legacy applications, and so on. Maritime systems fall into this category, since they exhibit certain properties that make internal software auditing (for correcting bugs) challenging. Several of the systems used in maritime transportation are custom, based on legacy software, and hard to update. Therefore, although there are no hardening techniques for maritime systems *per se*, most of the proposed hardening techniques are designed to be applied to systems similar to the maritime ones.

There are different techniques for system hardening. For old, typically applied to every system by default nowadays, to more advanced ones, like memory allocators, integrity solutions, randomization, attack-surface reduction (debloating), and trusted execution environments. Below, we provide a quick overview.

#### 7.6.1.3.1 Standard

In this category we have the hardening techniques that are considered standard, meaning that they are usually deployed by default when executing a program, unless declared otherwise. These hardening techniques are among the oldest ones developed and thus have been widely adopted.

Firstly, we have the Address Space Layout Randomization (ASLR) [PaX 2003] which is responsible for randomizing the process address space layout of an executing program. As a result, the addresses of the various modules of the program, such as the stack, heap and the libraries, are unknown and randomly loaded upon the execution of the program. For this reason, developing exploits for ASLR enabled systems is more demanding, even if exploitable vulnerabilities are in place, because the attacker needs to use other means to find the addresses of the programs (i.e. information leaks). Recently, ASLR schemes have been also designed for SGX environments [JBS 2017].

Next, we have the Data Execution Prevention [AA 2004], which separates the memory regions that are executable and non-executable, thus preventing the execution of newly injected code into a running program

through the user's input. As a result, even if an attacker successfully injects code into the stack, for instance, the execution will not work as the stack is by default a non-executable region.

Finally, we have stack cookies [CPM+ 1998], which protect return addresses on the stack from linear overflow. This defence crashes the program once the stack cookie is overwritten, since it realizes that a linear buffer overflow took place with the purpose of overwriting the return address of the function.

#### 7.6.1.3.2 Memory allocators

Many programs are still written in unsafe programming languages like C and C++, despite the various security weaknesses they may present. Some examples include unpredictable behaviour, crashes, and security vulnerabilities. One proposed hardening defence is by means of memory allocators that try to reduce the risk of the program being exploited by making various modifications regarding the memory of the program.

One example is the memory allocator *DieHard* [BZ 2006], which provides two features to defend programs against memory errors. The first one places the created objects randomly on a heap that is larger than the required one, in order to prevent an object from overwriting sensitive data. The second one runs multiple replicas of the program simultaneously, with different seeds for their randomized allocators. Then, while the programs are executing, it compares their contents and, if it finds that two replicas agree, that means that no memory error took place in order to overwrite any sensitive data. In contrast, if it detects that a replica uses data that the other replicas do not use, then it realizes that the specific replica has been exploited.

Another such example is *Cling* [Akritidis 2010], which is responsible for defending any dangling pointers, namely pointers that point to memory that has been deallocated, against use-after-free exploits. It does this by only allowing memory allocation reuse by objects of the same type.

In addition, *CETS* [NZMZ 2010], another memory allocator that utilizes instrumentation during compile time in order to detect all types of temporal memory safety errors (i.e. dangling pointers, double *free*'s and invalid *free*'s) in C programs during runtime. Basically, CETS adds two extra fields to each pointer, called *allocation key* and *lock address*, which are responsible for preventing a pointer from accessing a memory location that has been deallocated.

[ZAM+ 2021] propose an architecture, namely No-FAT, that builds on a recent trend in software: the usage of binning memory allocators. In particular, the authors observe that if memory allocation sizes (e.g., malloc sizes) are made an architectural feature, then it is possible to overcome many of the thorny issues with traditional approaches to memory safety such as compatibility with unsecured software and significant performance degradation. No-FAT incurs low overhead of 8% on SPEC CPU2017 benchmarks, and effectively mitigates certain speculative attacks (e.g., Spectre-V1) with no additional cost. Finally, when No-FAT is used for pre-deployment fuzz testing it can improve fuzz testing bandwidth by an order of magnitude compared to state-of-the-art approaches.

#### 7.6.1.3.3 Control-flow Integrity (CFI)

One of the most promising advanced hardening techniques is Control-flow Integrity (CFI) [ABEL 2009], originally proposed almost one decade ago. The technique statically analyses a program for creating an estimation of the legitimate Control-flow Graph (CFG) and enforces it at runtime each time an indirect branch takes place. In short, CFI computes all possible targets of an indirect branch. As a result, when an

attacker overwrites control data used in an indirect branch, it is constrained to follow only the legitimate targets that were previously computed. For example, changing the control flow of a program to point to a ROP (Return-oriented Programming) gadget is not possible, since such flow will never be part of the computed CFG. CFI has been realized in practice, especially for the forward edge, which includes constraining the targets of function pointers and VTable-based calls in C++ programs, and it now ships with standard compilers, such as Clang [Clang10].

Recently, [BCN+ 2017] systematically compared a broad range of CFI mechanisms using a unified nomenclature based on (i) a qualitative discussion of the conceptual security guarantees, (ii) a quantitative security evaluation, and (iii) an empirical evaluation of their performance in the same test environment. For each mechanism, we evaluate (i) protected types of control-flow transfers and (ii) precision of the protection for forward and backward edges. For open-source, compiler-based implementations, we also evaluate (iii) generated equivalence classes and target sets and (iv) runtime performance

#### 7.6.1.3.4 Code Pointer Integrity (CPI)

Another promising technique for defending programs against memory error exploits is Code-Pointer Integrity (CPI) [KSP+ 2014]. This technique firstly statically analyses the program in order to find any objects that contain code pointers or *sensitive pointers*, namely pointers that are responsible for the indirect branches of the program. Then, it separates the process memory of the program between the *safe* and the *regular* region and moves the aforementioned objects to the safe one. The *safe* region can be accessed through safe memory operations that have been checked either at compile time or at runtime. In contrast, the rest of the program is located in the regular region and no checks need to be accessed. CPI then instruments the program in order to ensure that all the sensitive pointers are located in the safe region, while also checking that any pointer dereference is legitimate. Consequently, when a sensitive pointer is dereferenced, CPI checks during runtime that it is safe and, as a result, it prevents any control flow hijacking attacks.

#### 7.6.1.3.5 Software Debloating

Software debloating is a recently proposed field of study with that is attracting increasing research interest, targeted at preventing code reuse attacks by performing code reduction in bloated software. Bloated programs are high-complexity software that supports several features, of which only a subset is needed by each user. In addition, the entire shared libraries are usually loaded into memory, but again only a subset of the available functionalities are necessary for a program's successful execution. This leads to security problems, as it gives adversaries a large attack surface that can be used either for finding vulnerabilities or for constructing gadgets that can be used for code-reuse attacks. To mitigate this threat, various code reduction techniques have been proposed over the years.

First, Koo et al. [KGP 2019] proposed a configuration-driven debloating technique that prevents shared libraries from being loaded into memory, based on the program's configurations. This is done by utilizing static and dynamic analysis in order to map each configuration directive to its corresponding library. This mapping is then used for instrumenting the program to prevent it from loading unused libraries when their corresponding configurations are disabled.

Quach et al. [QPY 2018] proposed a technique that performs software debloating by preserving the information that is produced during the program's compilation stage regarding the code dependencies of each functionality. This information is used in order to load only a subset of the required shared libraries for each corresponding functionality, based on the precomputed control-flow dependencies. The authors suggest that their technique improves the security of the debloated program, not only through the reduction of the attack surface, but also because of the increased effectiveness of other hardening techniques, such as CFI, that only need to analyse a smaller amount of code.

The above software debloating research relies on program source code, whereas the RAZOR framework proposed by Qian et al. [QHA+ 2019] uses control-flow heuristics to determine only the code that is necessary for the program to execute successfully, based on the user's utilized functionalities or related ones. This is done in three stages, RAZOR firstly records all executed code based on the user's sample inputs, then it finds related features that might not have executed on the current run but are still essential for the program's successful execution. Lastly, it rewrites a minimal version of the original binary, incorporating only the necessary code and excluding features that were previously ruled to be unused. The authors claim that this technique improves both the security and the performance of the debloated programs.

Finally, another debloating technique that does not require program source code and only targets binaries was proposed by Ghaffarinia and Hamlen [GH 2019]. This technique reduces the attack surface of bloated applications, namely high-complexity software, by restricting their available unused control flows. This is done by firstly creating a contextual control-flow graph (CCFG) based on the user's interactions with the program. This CCFG is then used to restrict functionalities that are not utilized by the users but exist in the binary. The code restrictions are enforced by instrumenting the jump instructions that target code that was previously computed to be unused by the users, based on the CCFG. This technique is not only effective towards preventing code-reuse attacks, as it reduces the code that an adversary could use as gadgets, but can also help remove possible vulnerable code that offers features unwanted by the users.

#### **7.6.1.3.6 Randomization**

Fine-grained randomization is a promising technique against Return-oriented Programming (ROP) attacks, as it applies randomization at the binary level of a program, as opposed to ASLR, which only randomizes the process layout and leaves the instructions static.

One such example is Instruction Location Randomization (ILR) [HNC+ 2012], which randomizes every instruction within a program. This is accomplished by assigning to every instruction a successor instruction, this enables ILR to randomly distribute the instructions across the memory. As a result, this changes the sequential model of the program to a non-sequential execution, as every instruction, regardless of its position, knows the next instruction to execute.

In addition, Pappas et al. [PPK 2012] proposed a methodology that applies in-place randomization at the binary level. This is done by substituting and reordering instructions within a code block, and also by reassigning the registers of the program. Consequently, this achieves instruction diversification inside a basic block; as a result, it manages to probabilistically break 80% of instruction sequences that could be potentially used for ROP attacks.

Oxymoron [BN 2014] is a fine-grained memory randomization technique that not only aims to defend programs against just-in-time (JIT) ROP attacks, but also tries to prevent memory overhead that other fine-

grained randomization methodologies might present. This is done by randomizing the instructions in such a way that they can be accessed by other processes as well, something which is not the case with other similar solutions that make code sharing among processes difficult. The randomization starts by assigning a unique label to the code and data of the program and thus enabling the code sharing, as the code can be accessed by utilizing the unique labels instead of randomization-dependent addresses. Finally, the code is split into pieces that each contains a single memory page, which are then randomly loaded and shared among the processes.

Recently, [KCL+ 2018] present compiler-assisted code randomization (CCR), a hybrid approach that relies on compiler-rewriter cooperation to enable fast and robust fine-grained code randomization on end-user systems, while maintaining compatibility with existing software distribution models. CCR augments binaries with a minimal set of transformation-assisting metadata, which a) facilitate rapid fine-grained code transformation at installation or load time, and b) form the basis for reversing any applied code transformation when needed, to maintain compatibility with existing mechanisms that rely on referencing the original code.

The literature reviews the main security hardening techniques abovementioned that are applicable to the maritime systems. Nonetheless, there is a growing need to deploy security hardening approaches that address system requirements specific to the maritime sector.

#### **7.6.1.3.7 Trusted Execution Environments (TEE)**

Trusted Execution Environment (TEE) is a tamper-resistant processing environment that runs on a separation kernel. It guarantees the authenticity of the executed code, the integrity of the runtime states (e.g. CPU registers, memory and sensitive I/O), and the confidentiality of its code, data and runtime states stored on a persistent memory. In addition, it shall be able to provide remote attestation that proves its trustworthiness for third-parties. The content of TEE is not static; it can be securely updated. The TEE resists against all software attacks as well as the physical attacks performed on the main memory of the system. Attacks performed by exploiting backdoor security flaws are not possible.

Generally speaking, a lot of technologies that implement TEE in modern processors exist, some of them including the following:

- Arm's TrustZone [PS 2019] technology offers an efficient, system-wide approach to security with hardware-enforced isolation built into the CPU.
- MultiZone Security is the first trusted execution environment for RISC-V created by Hex Five Security.
- The AMD Platform Security Processor (PSP), officially known as AMD Secure Technology, is a trusted execution environment subsystem incorporated into AMD microprocessors.
- Intel Software Guard Extensions (SGX) is a set of security-related instruction codes that are built into some modern Intel CPUs that could be used to implement a TEE.

- Apple uses a dedicated processor called SEP (Secure Enclave Processor) for features like data protection, Touch ID, and Face ID. The SEP is responsible for handling keys and other information such as biometrics that is sensitive enough to not be handled by the application processor.

The literature reviews the main security hardening techniques abovementioned that are applicable to the maritime systems. Nonetheless, there is a growing need to deploy security hardening approaches that address system requirements specific to the maritime sector.

#### 7.6.1.4 Maritime communication system security and trust infrastructures

The state of the art in security, specifically for Maritime Transport communication systems, is as follows.

##### 7.6.1.4.1 Secure communication

As shown by Rødseth et al. [RFM+, 2020], there is a diverse set of communication interactions in shipping, such as:

- Ship-to-ship
- Ship-to-port
- Ship-to-Remote Control Centre (RCC)
- Ship-to-Vessel Traffic Services (VTS)
- Ship-to-Application Service Provider (ASP)
- Ship-to-Medical Aid Provider (MAP)
- Ship-to-Search and Rescue (SAR)
- Ship-to-Maritime Rescue Coordination Centre (MRCC)

As depicted in Figure 16, these interactions can make use of a variety of communication channels, depending on factors such as available technology, infrastructure, costs and local conditions. Commonly used today is SatCom (blue lines), either via low earth orbit (LEO, for instance VSAT or low-directional Inmarsat services) or geostationary earth orbit (GEO, for instance Iridium or VHF) to a satellite application service (SAS) and further to shore entities over land lines (green lines). While docking and close to shore, ships are likely to use traditional land-based channels, such as WiFi, Ethernet and GSM/LTE/5G.

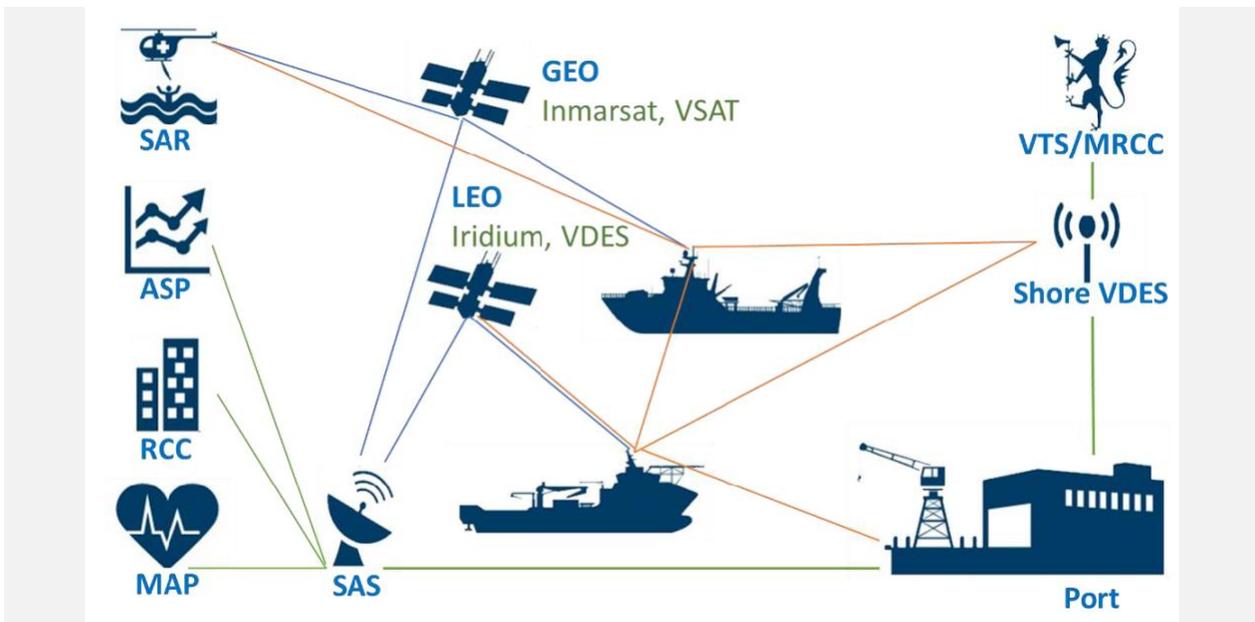


Figure 16. Examples of maritime communication channels

A lot of the direct communication between ships and ships and land services can be replaced with VDES (orange lines), but it is vital that the security mechanism on top of this is economically, technically and politically feasible. The use of a public key infrastructure (PKI) is a common way of realising this, and within the maritime domain we can find established solutions using this technology (reproduced from Rødseth et al.):

- The Long Range Identification and Tracking (LRIT) system [IMO 2020] collects position reports from ships worldwide and make them available to coastal states. A PKI operated by IMO secures communication between the distributed LRIT data centres.
- SafeSeaNet [EMSA 2020A] is a system similar to LRIT, but operated by the European Maritime Safety Agency (EMSA) and covering much more detailed information about ship movements and port calls.
- The International Hydrographic Office (IHO) also operates a type of PKI [IHO 2015] that is used to encrypt and verify the authenticity and integrity of electronic charts.

Among solutions that are on the way to being established, we have the following:

- The Maritime Connectivity Platform (MCP) [MCP 2020] intends to establish a PKI to provide a communication system for the maritime industry, including an identity registry, a service registry and a messaging service.
- *ISO/TC 8 Ships and marine technology* has proposed that a PKI should be used by the issuing party to digitally sign ship certificates [IMO 2017A].

### Communications Architecture for Autonomous Passenger Ship

The communication architecture of the autonomous passenger ship (APS) enables communication in its operational context through a heterogeneous group of different technologies, as shown in Figure 17. It enables the APS to perform ship-to-shore communication with a remote-control centre (RCC) to carry remote navigation and control functions. It also enables ship-to-ship communication to support safe navigation functions. In addition, it enables emergency communication to carry emergency navigation and control functions by an emergency control team (ECT).

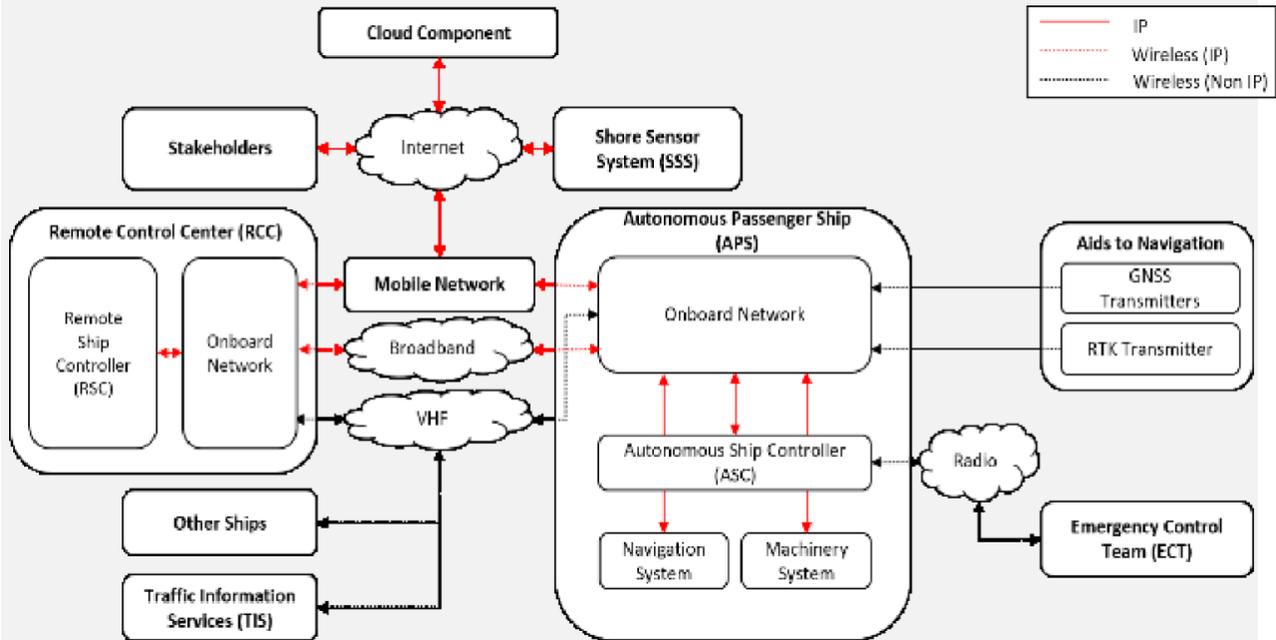


Figure 17: Overview of the APS Context

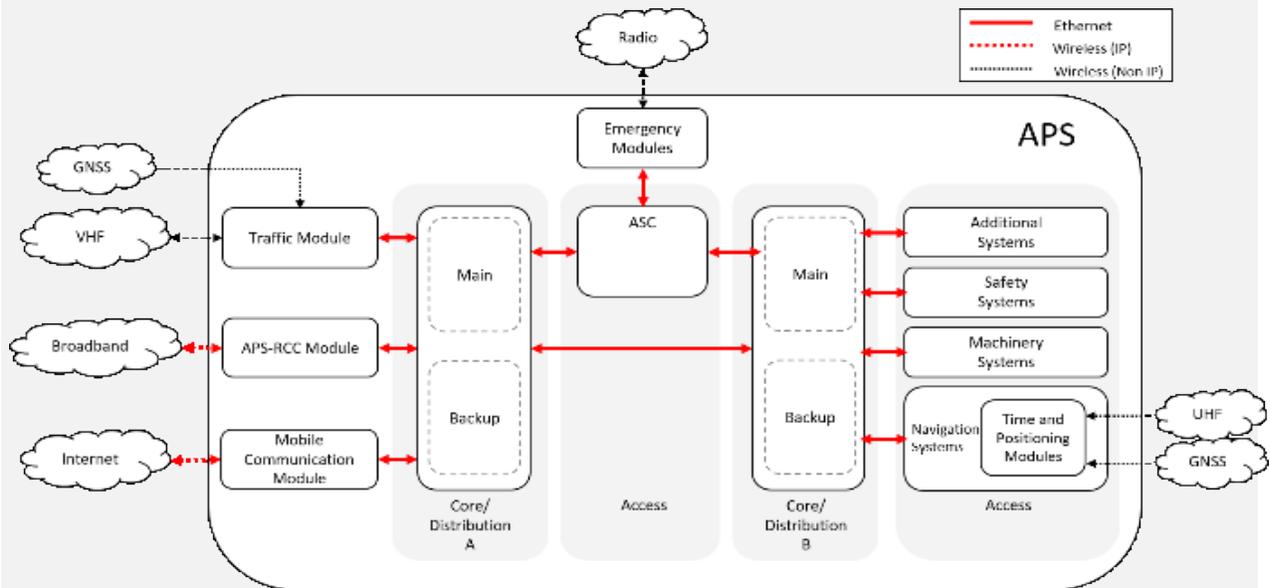


Figure 18: On-board network architecture

Additional capabilities to facilitate the management of the APS systems and facilitate stakeholders' communication can be provided through a cloud component. In this respect, internal communication is

supported by an on-board network, as shown in Figure 18. There are six main communication gateways in the APS. In particular, there are two IP based gateways for ship-to-shore communication utilizing several implementation solutions, such as mobile communication (4G/LTE/5G) and wireless local area networks (WLAN) technologies. The third gateway supports ship-to-ship communication through an automatic identification system (AIS). The fourth gateway carries emergency communications, while the fifth and sixth gateways are utilized to receive signals for real-time kinematic (RTK) and global navigation satellite system (GNSS) communication. The internal network architecture is designed to provide redundant communication paths, a segregated network and secure communication. A group of servers called the autonomous ship controller (ASC), hosting centralized monitoring and controlling capabilities, is interfaced with two network traffic core and distribution tiers (C/D). Each tier consists of main and backup switches with IP routing capabilities. C/D tier A connects the external gateways with the servers in the ASC, while C/D tier B connects the secondary servers in the ASC with the internal and segregated sub-networks. A centralized connectivity manager is responsible for performing network management functions, such as configuring and monitoring the network devices, in addition to security related functions. The detailed communication architecture is described by Amro et al. in [AKLT 2020].

Overall, the depicted diverse set of communication interactions in the shipping industry is an emerging trend that requires continuous investigation.

The applicability of the aforementioned communication architecture is specific to an inland waterway use-case. Many new communication challenges have arisen and will arise in the future, depending on the degree of autonomy considered for the ship and its operational environment, such as for transnational operations, and to sail on the high seas or in the Arctic regions. These challenges need to be investigated, and the outcomes well tested before they are integrated into autonomous maritime transport.

Several studies [RKP+2013] [HHK+ 2017] have investigated and proposed promising communication and networking architectures/technologies for this purpose. The communication architecture for an unmanned merchant ship developed by Rødseth et al. [RKP+ 2013] used the baseline case from MUNIN [MUNIN 2016]. In this, the authors elicited and analysed the different operations in autonomous ships that potentially need communication, and their respective requirements for that communication. In addition, they also presented the relevant communication systems that could apparently meet the specified needs. Next, Höyhty et al. [HHK+ 2017] studied the connectivity challenges of autonomous ships in different environments, for use-cases such as operating in shoreline or port areas, deep seas, and the Arctic regions. At the same time, they also reviewed the possible communication options for the use-cases. Finally, a hybrid communication architecture was proposed that primarily focused on these four components: i) essential ship data, ii) sensor fusion and connectivity management, iii) connectivity management, and iv) safety, security and avoidance of interference. The main recommendation of the architecture is to utilize both terrestrial and satellite communication systems, and to use multiple redundant systems if necessary to ensure resilient operations.

At present, very few communication options are available for maritime transport; they are mainly limited to satellite systems, or other long-range and low-bitrate communication systems [AMY+ 2018] [ZPK+ 2019]. Furthermore, some of these options that are applicable in manned ships could not meet the needs of autonomous maritime transport [AMY+ 2018] [ZPK+ 2019] [HM 2020]. For example, to run a ship in remote-control mode requires the ship to perceive the environment (capture information using sensors,

cameras, radars, and LIDAR) and transmit the relevant navigational data/situational awareness to RCC in real-time. In order to support this, communication systems must satisfy criteria that include high security, data integrity, bandwidth capacity, latency (real-time communication) and continuous connectivity (uninterrupted communication between RCC and the ship), at the very least. In addition, the systems should be cost-effective in terms of both price and energy efficiency. In contrast, most of the existing options satisfy only some of the properties. For instance, satellite communication systems support limited bandwidth and are also expensive in terms of both finance and energy efficiency [ZPK+ 2019]. Although the financial cost will be reduced with the growth in supply, the cost of communication will still remain an important constraint for autonomous ships [RKP+ 2013].

As a potential alternative, cellular communication (mainly 5G and sometimes 6G currently under development) has recently been widely investigated [POM 2020] [HM 2020]. Indeed, this can be an efficient, flexible and secure communication option for ship-to-shore communication (APS-RCC communication); however, only in near-coastal waters and inland waterways with RAN (Radio Access Network) coverage [POM 2020]. In the regions without RAN coverage, the APS still has to depend on other communication options. Even for on-board communication, depending on the 5G mobile national infrastructure may not be feasible, leaving only the option of establishing a private 5G network on the ship itself [POM 2020]. However, setting up a private 5G network entails various regulatory challenges related to frequency allocation, which will need to be addressed.

Nonetheless, the authors [RKP+ 2013] mentioned that considerable progress on the technical concepts of autonomous ships' communication systems should be expected to occur. In order to achieve that, some relevant concepts open for further investigation are hybrid satellite-terrestrial systems (different communication systems for coastal regions and on the high seas), sensor data fusion and transmission (to reduce data transmission bandwidth need), redundant communication systems (to ensure maximum availability and accessibility), ship mega-constellations (satellite mega-constellations providing global connectivity), and multi-hop connectivity (a mobile *ad hoc* network with multi-hop features among hundreds of ships) [HHK+ 2017]. These communication concepts could potentially address many of the challenges faced by autonomous maritime transport. Alternatively, satellite services such as Iridium Next, a Low Earth Orbit (LEO) system, and a High Elliptical Orbit (HEO) satellite covering Pan-Arctic regions, are other considerable options for the purpose [ZPK+ 2019]. However, to adopt different relevant communication systems, the legal and commercial challenges accompanying them are equally important and must be addressed.

#### **7.6.1.5 Secure autonomous ships**

Several studies have proposed and discussed risk assessment methods before and during the early development stages of autonomous ships. Kavallieratos et al [KKG 2018] proposed a multilayer architecture for ICT systems in cyber-enabled ships (CE-S), which include autonomous ships. The authors then applied the STRIDE threat-modelling method to identify potential threats. The associated risks were then assessed using risk matrices inferred from the work of Jelacic et al. [JRL+ 2018]. In addition, Tam and Jones applied a model-based risk assessment framework called MaCRA [TJ 2019] on three futuristic ships with different applications and levels of autonomy. The process was started by applying the MaCRA threat assessment framework and then the risk assessment process. Other studies analysed the risks associated with cyber threats, considering their impacts on safety. The safety impact of cyberattacks against autonomous inland ships has been discussed by Bolbot et al. [BTB+ 2020]. The authors leveraged a cyber preliminary hazard

analysis (PHA<sup>331</sup>) method, considering the known vulnerabilities in existing systems, in addition to analysing potential cyberattacks that could impact the safety of vessels, as well as possible countermeasures. Further, a joint safety and security analysis of a proposed architecture for an autonomous passenger ferry was conducted and presented by Amro et al. [AGK 2019]. The analysis was conducted by facilitating the six-step model (SSM) initially proposed by Sabaliauskaite et al [SAM 2016]. Given the lack of sufficient statistical information to quantify the likelihood and impacts of cyberattacks against autonomous ships, all the observed risk analysis approaches are qualitative.

More recent research efforts include the work of Chang et al. [CKY+ 2021], who proposed a risk assessment method for maritime autonomous surface ships. To achieve this, they drew on a literature review, expert opinion and Formal Safety Assessment. Among the different risks identified, cyberattacks take a prominent position. The proposed risk assessment method is based on Failure Modes and Effects Analysis (FMEA), in conjunction with Evidential Reasoning (ER) and a Rule-based Bayesian Network (RBN), to quantify the risk of the identified hazards, which include human errors, interaction with manned vessels, detection of objects, interaction with the physical environment, system failures, cyberattacks and equipment failures.

An assessment process consisting of three phases, assessment preparation activities, assessment conduct and communication of results, was developed and a quantitative cyber risk analysis was conducted for the evaluation of a vessel's cyber risks by Svilicic et al [SKR+ 2019]. However, it cannot be performed prior to the actual system testing as it does not engage autonomous ship operations [BTB+ 2020]. A risk analysis process of functional software failures, their propagation, and incorporation of the results in traditional risk analysis methods, such as fault trees and event trees, demonstrated through a case study of a decision support system for an autonomous remotely operated vehicle, is presented in Thieme et al [TMU+ 2020]. Such examples, with significant 2020 checkpoints, exemplify different future autonomous ships and promote knowledge of maritime cyber-risks and vulnerabilities, against cutting-edge sensor networks and remote access. There is limited work on machine-learning methods driving the risk assessment process, utilizing both historical and real-time data to provide insights into traditional risk assessment techniques, as applied in specific industries, such as automotive [HR 2020]. In addition, there is a strong requirement to increase safety regulations and improve the general technological understanding of complex automated system behaviour [BLW 2017].

Autonomous ships are characterized by the increasing deployment of interconnected cyber-physical systems. To this end, a comprehensive requirements elicitation process requires a security assessment to incorporate safety aspects. Existing surveys studied such security and safety co-engineering approaches [Abulamddi 2017; KKG 2020]. Specifically, Cui and Sabaliauskaite in [CS 2018] proposed the US2 method to analyse safety hazards and security threats with a view to identifying security and safety requirements. Further, the Failure Attack CounTermeasure (FACT) approach is proposed in [CS 2017] to identify the necessary security and safety controls and barriers for contemporary CPSs. N. Guzman et al. in [GKK+ 2019] suggested the Uncontrolled Flows of Information and Energy (UFoIE) model to study interdependencies between the CPS components and analyse the security and safety risks as a means of eliciting requirements. Finally, G. Kavallieratos et al. in [KKG 2020] proposed a security and safety

---

<sup>331</sup> PHA stands for Preliminary Hazard Analysis

requirements co-engineering approach based on predefined security and safety objectives, also providing a use case for an autonomous vessel. Focusing on the engineering methods used to meet security requirements, various surveys can be found in the literature [NNY 2010; PKG 2017]. These cover the pros and cons of the surveyed methods and examine their appropriateness for contemporary application domains. H. Mouratidis et al. proposed the Secure Tropos methodology [MG 2007] to systemically analyse systems under development to enable security by design. Using Secure Tropos, domains where the application of interconnected CPSs is prominent have been studied. In particular, the industrial internet of things [MD 2018], autonomous cars [PHL+ 2018] and autonomous ships [KDK 2020] have been analysed.

In recent years, the safety and security of autonomous ships have attracted much attention. As argued by Torkildson et al. [TLJ+ 2018], most studies have co-analyzed security together with safety, apart from some that focused specifically on only security concerns for autonomous ships.

Rødseth and Burmeister [RB 2015] performed the risk assessment for MUNIN, using a risk-based method for the design and analysis of an “industrial autonomous system” that was based on Formal Safety Analysis.<sup>332</sup> Unlike other investigators, they also recommended conducting a cost-benefit analysis as a part of risk assessment. Finally, to improve the quality of the MUNIN system, ease the task of risk assessment and make the system cost-effective, the study suggested keeping the complexity of the system as low as possible. Similarly, there are two studies by Fan et al., [FWM+ 2020] and [FMZ 2021], in which the same group of authors proposed frameworks for the identification of risk-influencing factors (RIFs) and quantification of the RIFs in MASS, respectively. In the earlier study, they used a literature review for the identification of RIFs in remotely controlled (or crewless) MASS, followed by the use of an expert opinion method to validate the identified RIFs, as well as elicit new RIFs if any were missing. Then, in the later study, they utilized the concept of Risk Priority Numbers (RPNs), adopted from Failure Mode and Effects Analysis, to measure the risk level (or to quantify risks) for MASS. The parameters required to define the RPNs are obtained using expert knowledge. Finally, they have applied and demonstrated the framework in a prototype MASS that has been under trial since October 2019.

Some studies have focused on analysing specifically the cybersecurity concerns of autonomous ships. Silverajan et al. [SON 2018] identified the main attack surfaces through which attackers can gain unauthorized access to or disrupt the operations of a smart ship. Further, the authors showed how attackers could employ six popular cybersecurity attacks (code injection, tampering and modification, GPS spoofing, AIS spoofing, signal jamming, and communication link eavesdropping and disruption) to exploit those surfaces. To mitigate the security issues, they proposed defence strategies that mainly involved traditional countermeasures commonly in use. Next, Shipunov et al. [SVN+2019] expanded a Maritime Cyber-Risk Assessment (MaCRA) model and used it to assess the cyber risks on crewless ships. They also demonstrated their model theoretically in three crewless vessel projects. Finally, Furumoto et al. [FKS+ 2020] identified and discussed attack scenarios that can be used for cybersecurity risk management. Considering the threat surfaces, they proposed a secure ship network topology that uses technologies and concepts including SDN, machine learning, and zone-based topology for the realization of autonomous ship operations. The authors

---

<sup>332</sup>Marin Insight, What is Formal Safety Assessment in Shipping? <https://www.marineinsight.com/marine-safety/what-is-formal-safety-assessment-in-shipping/>

advocate integrating security into the design (security by design) of the ship and applying risk management when the ship comes into service.

Perhaps because autonomous ships are still in the development phase, most studies depend on easy-to-use and less resource-constraining techniques to elicit risks (or safety and security requirements)—for example, literature review and expert opinion. However, a major drawback of these techniques is their ineffectiveness in the elicitation of “unknown-unknown” requirements (i.e. requirements that are not expressible, articulated or accessible, but are still potentially relevant). Failure to identify the “unknown unknowns” concerning safety risks (that are unknown to the engineer and specialist) can have severe consequences [JES 2017]. Especially for a new and emerging area like an autonomous ship (with an amalgamation of many technologies and concepts such as IoT, machine learning, big data, cloud services, automation, etc.), where security concerns directly involve the safety of human life (in the case of a passenger ship) and property (in the case of a cargo ship), “unknown unknown” risks should not be neglected. Achieving that requires the implementation of more creative and exploratory elicitation approaches: for example, prototypes, scenarios, workshop techniques, and their combinations with other techniques that also have the ability to detect “unknown unknown” risks [SS 2013].

In addition, some studies have adopted the same approach for both cybersecurity and safety risk assessment. It is necessary that they distinguish between these two. Safety hazards are relatively known quantities and can be described in terms of probabilities and the engineering sciences, whereas cybersecurity threats are posed by actors who are willing and able to learn and adopt new methodologies [McDougall 2017]. Therefore, researchers must understand that the approach taken within the realm of safety may not be an exact fit for cybersecurity, so they should consider alternative relevant approaches for their assessment purposes.

Last but not least, these studies focused on and discussed primarily the traditional cybersecurity threats. Certainly, an autonomous ship will be vulnerable to those threats and require remedies. However, along with them, equal attention should be paid to new cybersecurity threats that will be introduced by the integration of various advancing ICT technologies and concepts in maritime transport.

#### **7.6.1.6 Resilience in critical (maritime) infrastructures**

Several definitions for critical infrastructure resilience are available in the literature and some of them are indicatively presented below [SK 2019]. According to the US National Infrastructure Advisory Council [BWC 2010], infrastructure resilience is “the ability of critical infrastructure systems, networks, and functions to withstand and rapidly recover from damage and disruption and adapt to changing conditions.” Resilience can be measured based on four main features [BWC 2010]: robustness, i.e. the ability to keep operating in case of interruptions, including those caused by low probability but high impact events; resourcefulness, i.e. the ability to effectively manage a disaster and prioritize mitigation controls in case of damage; rapid recovery, i.e. the ability to quickly restore normal operation; and adaptability, i.e. the ability to absorb the consequences of a disaster.

A similar definition is given by the UK Cabinet Office [CO 2011], where the main characteristics of resilience are defined as: resistance, i.e. enhancing the strength or protection of the infrastructure by minimizing the potential impact; reliability, i.e. inherently design the system to operate in abnormal events; redundancy, i.e. design the infrastructure with spare and/or backup parts; and response and recovery, i.e.

ensure the fast and effective recovery from disruptions. These definitions ultimately correspond to similar requirements provided by Kotzanikolaou et al. [KTG 2013]. For example, robustness, defined by Berkeley et al [BWC 2010], is closely related with resistance, suggested by the UK Cabinet Office [CO 2011]. Through this analysis, the definition given by [CO 2011] will be adopted and the terms robustness and resistance will be treated as synonymous. It is important to note that resilience and cost optimization are contradictory requirements. Since resilience implies properties like redundancy and robustness of the infrastructure, it is obvious that a resilient infrastructure will not be optimal in terms of cost. However, an interesting problem is to concurrently achieve both properties: a balance between infrastructure resilience and cost optimization. The result will be a suboptimal solution, which will offer adequate resilience, with the minimum cost overhead in comparison to the optimal cost solution.

As resilience relies on several properties (resistance, reliability, redundancy, response), it can also be considered as a “derivative” security property that relies on the combined application of various security services, including among others the early detection of threats, system hardening, communication reliability and trust management. Towards this direction, Grigoriadis et al [GPK+2021] describe the initial validation results of the CyberSecurityForEurope maritime transport demonstrator. There, various security services for threat modelling, risk assessment, system hardening, communication security and trust management for maritime systems have been integrated and tested. Such integrated security solutions may enhance the resilience of critical maritime systems.

## 7.6.2 SWOT Analysis

A SWOT analysis has been conducted for the maritime transport sector as follows. The highlights of this swot analysis are addressed in Figure 19.



Figure 19: Maritime Transport SWOT Summary

### 7.6.2.1 Strengths

- Maritime transport is a **critical industry sector** of the EU economy that is considerably reliant upon the maritime movement of cargo and passengers [CMB+ 2011] and is characterized as a “blue economy” established and emerging sector [EC 2019].

- “**Blue growth**” is considered a long-term strategy to support sustainable growth in the marine and maritime domain as a whole and it is recognized as the **maritime contribution to deliver the goals of the Europe 2020 strategy for smart, sustainable and inclusive growth** [EU 2020]. In this vein, it is highly important to ensure the security and safety of maritime transport. Digitalization [DNV GL 2020] has taken over in the maritime transport operations in a highly evolving trend [DNV GL 2020] that increasingly attracts the attention of threat agents (i.e. terrorists, cyberwarriors, political/nation-state adversaries, hacktivists, competitors, etc.), as thoroughly described in Section 7.4.1, to commit sophisticated cyberattacks. As a consequence, the protection of the maritime digital infrastructure becomes of vital importance on a global scale.
- On account of this, research initiatives have been established in the EU in the area of secure maritime transport (universities, R&D projects and industry). For instance, during the last decade, the **EU has funded a series of remarkable, innovative EU R&D projects** that fortify and prove the European competitive advantage in maritime cybersecurity research. Such sector-specific cybersecurity research projects are indicatively as follows: the FP7 SECTRONIC project [SECTRONIC 2020] developed an integrated system for increasing the security of maritime infrastructures regarding ports, passenger transport and energy supply; the CIPS’12 CYSM project provided a collaborative cyber-physical security management approach concerning port infrastructures [PPK 2015]; the CIPS’14 MEDUSA project [PKP 2016] focused on identifying multi-order dependencies between port stakeholders to secure port supply chains; the FP7 MUNIN project [MUNIN 2016] introduced a technical concept for the operation of an unmanned merchant vessel to assess its technical, economic and legal feasibility; the H2020 MITIGATE project [KPMP 2018] aimed to contribute to the effective protection of ICT-based port supply chains; and the H2020 SAURON project proposed a holistic situational awareness concept to protect EU ports and their surroundings [SKP+ 2019].
- Such research initiatives, have addressed and analysed the maritime transport sector-specific security requirements and promoted **unexplored grounds of research** (such as security risk propagation in maritime transport environments, maritime security awareness in a holistic view in both cyber and physical planes, security in autonomous ships, etc.).

#### 7.6.2.2 Weaknesses

- There is a lack of collaboration in the EU maritime transport security initiatives. Most of the **technologies utilised in the maritime transport cybersecurity were not developed within the EU**. Modern maritime transport has evolved to use technology for tasks that were otherwise carried out using analogue means. Nevertheless, most of the technology utilized in the maritime domain is based on the technology used in computer systems in general, however, but with the right appropriate adaptation. Such technologies, such as operating systems, device firmware, and software applications, are largely designed and developed in software houses that are not based in the EU. This makes the analysis and security auditing of such systems hard, especially, considering that several of those systems are highly customized. Essentially, this means that the core expertise of their internals, which is valuable to the analyst, may not be easily readily available.
- Since such technologies aforementioned were not designed and implemented in the EU, their evolution **may not share the priorities imposed by the EU**

#### 7.6.2.3 Opportunities

- The lack of standardized technologies for secure maritime transport on a worldwide scale creates an opportunity for the EU to **promote digital sovereignty** in this area. In this vein, synergies are encouraged **to build common strategies and policies** towards EU maritime cybersecurity upon mutual collaboration.
- According to the UNCTAD 2020 Review of Maritime Transport report [UNCTAD 2020], some of the highest priorities for policy action that have to be considered in response to the current COVID-19 pandemic reality regarding the persistent challenges facing the maritime transport are **the promotion of greater technology uptake and digitalization**, harnessing data to satisfy monitoring and policy responses, and increasing the focus on agile and resilient maritime transport systems. To this end, the EU has an inherent opportunity to **invest in maritime cybersecurity efforts** (i.e. maritime risk management and maritime event/disaster management) that will **accelerate and promote the EU's growth and recovery policy**.
- The focus on implementing crisis management strategies and recovery action plans could generate a comparative advantage at international level to **reshape the global economy**.

#### 7.6.2.4 Threats

- The threat landscape related to cyber and physical attacks in the maritime transport is continuously evolving as presented in section 7.3. This rising **threat landscape evolves exponentially** and despite the continuous effort for security technological progress in this area, it appears really **difficult to catch**.
- Considering what mentioned above, the **development of security technologies that may be "outdated" too soon**. For this reason, valuable assets of Critical Information Infrastructures of Maritime Transport, such as SCADA systems, AIS systems and ECDIS platforms are likely to be more targeted.
- Nevertheless, the growing trend of using **emerging technologies**, such as Cloud-based systems, Big Data, IoT, Deep Learning and adversarial learning techniques, machine learning, augmented reality, distributed ledger technologies and AI-based tools in maritime transport systems could generate new emerging threats as such technologies **are still a new area of investigation** and cannot yet be fully explored; thus, such supporting systems cannot be fully protected.

#### 7.6.3 European Digital Sovereignty

Developments in digital sovereignty on a global scale over the last few decades have given ICT an emerging role in maritime transport for promoting transparent interactions among maritime stakeholders and facilitating their collaboration through compound and heterogeneous dispersed interconnected networks [KAP+ 2018]. This complex cyber-dependent nature of maritime critical infrastructures has entailed limitations in the provision of security awareness and challenges skilled adversaries to intrude on such networks by carrying out sophisticated attacks with high-level intelligent techniques [KPMP 2018]. In this vein, the preservation of information security enablers, the CIA triad (Confidentiality, Integrity and Availability) along with the insurance of other properties, such as authenticity, accountability, non-repudiation, and reliability [ISO/IEC27000 2018], in maritime transport's critical infrastructures becomes a tough task to implement, which raises the possibility of the occurrence of unwanted security events (i.e. attacks, mishaps, damage, disruption or failure).

Setting a common EU cybersecurity research roadmap for the maritime transport sector that will boost the resilience of critical maritime systems, protect digital communication among maritime transport key-players by creating a circle of trust, and reinforcing the security of the inherent cyber-dependencies of the dispersed interconnected maritime critical infrastructures will assist in building a competence network that will raise cybersecurity preparedness, facilitating data security and digital safety in Europe. The development of such a network will amplify Europe's strategic autonomy, namely its ability to act independently in the digital world [EPRS 2020; Gueham 2015] and reinforce its agility against digital security challenges.

#### **7.6.4 COVID-19 and Public Health Dimension**

The COVID-19 outbreak has impacted human life and economy on a global scale. Since the start of the COVID-19 crisis, the European Commission, the Member States and the shipping industry have undertaken measures to safeguard the continuity of operations and therefore ensure the security of supply, as the situation is becoming more critical and could have tremendous consequences in long-term [EMSA 2020B]. In this vein, EMSA has implemented methods to analyse vessel traffic data and thus identify the shipping activities related to the pandemic disease in order to support the EU recovery strategy for managing the economic crisis and to assist all parties involved (EU, maritime administrations and shipping industry) [EMSA 2020B]. Within this framework, EMSA has recently conducted a vessel traffic survey based on port calls, which has reported an increased number of ships at anchor in comparison with 2019, especially in the case of cruise ships, passenger vessels and chemical tankers [EMSA 2020B]. The lockdown measures in various Member States due to the COVID-19 outbreak have restricted the movement of passengers and crew members and has reduced, though not stopped, international trade. Regardless of the hard pandemic situation, commercial vessel operations continue with the shipment of goods. According to the EMSA survey [EMSA 2020B], port calls from Europe to China regarding general cargo, gas carriers and bulk carriers have risen during 2020 compared to 2019. This highlights the strategic importance of maritime transport in the European and global market. Maritime shipping services, such as the transport of food, energy and medical supplies between continents, [Macola 2020], still remain undisrupted and play a critical role within the EU economy.

The pandemic COVID-19 disease has increased the trend towards teleworking in maritime transport. Because of the limited travel possibilities, a lot of on-ship inspections and maintenance must be done remotely. To maintain these activities undisrupted, digital operations have been significantly increased in the maritime transport sector. According to [Macola 2020], the pandemic is acting as a catalyst in the digital engagement of the maritime industry, introducing a concrete and stable digital workforce that could be gradually adopted for shipping operations and transactions in the long term [Macola 2020]. A rise in the use of dispersed interconnected critical information infrastructures in the maritime transport sector increases the cyber attackers' appetite to hack and compromise key assets, as argued previously in section 7.3. Given the globalization of the sector, all categories of attackers are possible.

New emerging technologies will pose new threats to the maritime ecosystem (analysed in section 7.3). According to the UNCTAD 2020 report on Maritime Transport [UNCTAD 2020], cybersecurity has been a burning issue in view of the COVID-19 pandemic. In particular, cyberattacks in the maritime transport domain were exacerbated by the poor ability of shipping enterprises and port stakeholders to protect themselves sufficiently in light of travel restrictions, social distancing measures and economic recession [UNCTAD 2020]. During the COVID-19 pandemic, Naval Dome (an Israeli cybersecurity company) has reported a 400% rise in cyberattack activity towards the new remote-working conditions, especially between

February and May 2020, involving ransoms, malware and phishing attacks [SafetyatSea 2020]. Maritime transport was one of the industries affected by hits from skilled cyber criminals [SafetyatSea 2020]. Remarkable examples have been published, including an email phishing attack to deliver malware or phishing links to compromise vessels and/or stakeholders' organizations [PWC 2020]. Some of these represent themselves as the World Health Organisation, whereas others use real vessel names and/or COVID-19 to impersonate actual ships raising emergencies related to infected crew and vessels via malware e-mail attachments [PWC 2020]. Another cyberattack alert has been raised from the Mediterranean Shipping Company (MSC), which has reported experiencing a network outage after a malware attack that compromised their official website and customer portal, which in turn affected online bookings for several days. The Danish pump maker DESMI was subjected to a blackmail attack, with the enterprise refusing to pay the ransom for compromised and unavailable data [PWC 2020]. To hinder the attack, the organisation shut down a few of its systems, including e-mail accounts, which eventually impacted their operations for a number of days [PWC 2020]. In addition, an uptick in cybersecurity incidents was claimed by SAS and BIMCO [SafetyatSea 2020].

Therefore, maritime transport companies need to be more agile, adaptable and better prepared for the evolving remote working brought about by the COVID-19 pandemic, and must stay focused on developing and implementing effective response strategies and plans that will boost maritime resilience.

In terms of COVID-19 and considering the health and safety of people involved in the maritime transport environment (passengers, sectorial stakeholders, etc.), domain specialists can utilise secure and trusted digital sources (e.g. public health related reports, information channels, teleconference platforms) to communicate information to maritime transport employees on COVID-19 disease, communicate the consequences towards domain's physical and cyber security, and share related information. In addition, maritime awareness remote training programs could be conducted to raise people's knowledge about coronavirus disease and guide them to implement proactive measures and response plans to limit the spread of the pandemic (e.g. adopt shipboard measures to limit COVID-19 risks, follow measures to manage embarkation and disembarkation during the pandemic, provide decision making for on-board suspected or confirmed COVID-19 cases, post port entry restrictions, promote hygiene measures, etc.). For instance, the International Chamber of Shipping released in June 2021 the 4<sup>th</sup> Edition of "Coronavirus (COVID-19): Guidance for Ship Operators for the Protection of the Health of Seafarers"<sup>333</sup> under the World Health Organisation's (WHO) International Health Regulations (IHR).

### 7.6.5 Green Deal and Climate Change

By 2050, the IMO aims to reduce the total greenhouse gas emissions associated with international shipping by at least 50% compared to 2008, regardless of maritime trade growth. This strategy was agreed by every IMO Member State, including all EU Member States that are participating in the IMO MARPOL Convention, and is aligned with the EU green deal. This is a challenging objective, and reducing greenhouse

---

<sup>333</sup> International Chamber of Shipping, Guidance for Ship Operators for the Protection of the Health of Seafarers, Marisec Publications, <https://www.ics-shipping.org/publication/coronavirus-covid-19-guidance-fourth-edition/>

gas emissions will require radical changes throughout the maritime sector at both technical and operational levels, including the development and implementation of new technologies, infrastructure and supply chain practices. These include the development of new fuels, changes to structural elements, efficiency improvements to monitoring and control elements in energy management and propulsion, but also voyage optimization through enhanced fleet management and logistics. Additionally, changes may be applied to existing supply chains, for both the procurement of ships and their use, such as the ongoing transition to fully electric and autonomous modes of operation, especially for smaller ships sailing on short routes (short sea shipping).

Maritime security does not affect climate change directly; however, maritime accidents, which can also happen as part of cyberattacks, can, in some cases, cause harm to the environment (e.g. oil slicks). In this vein, the illegal activity of threat actors targeting the maritime transport sector can impact the environment [GM 2019]. Just as the proliferation of weapons of mass destruction can raise chemical, biological, radiological and nuclear (CBRN) threats, so unauthorized exploitation of natural and maritime transport resources, (e.g. accidental or illegal LNG discharge due to manipulation of a compromised LNG monitoring system by cyber attackers [KPMP 2018]). For instance, piracy in the Gulf of Guinea created the most dangerous maritime zone in 2020, as attacks on oil tankers increased exponentially, leading to environmental degradation<sup>334</sup> and threatening the health of coastal communities. Although no major incidents linked to cyberattacks have been documented so far, we anticipate that having secure infrastructures in modern ships can ensure the uninterrupted operation of maritime transportation. Therefore, potential accidents that can harm the environment can be reduced.

Nevertheless, climate change risks (e.g. heat waves, floods and rising sea levels) can cause serious damages to maritime transport CIs and generate vulnerabilities for malicious actors to exploit, creating opportunities for them to launch cyberattacks on maritime ICTs<sup>335</sup> and thereby take advantage of the interconnected maritime transport cyber-physical systems.

The EU Maritime Security Strategy (EUMSS) [EC 2014; EC 2020B] stresses possible links to the impact of climate change on maritime security [GM 2019]. Additional effort is primarily needed to enhance research into the impact of maritime transport cybersecurity on climate change, and to propose mitigation actions and recovery plans to increase the cyber resilience of maritime transport CIs.

### 7.6.6 Impact on Democracy

Maritime transport is continuously adopting and adapting to new age and to the Information and Communication Technologies. This digital transformation is intended to make the sector more connected, integrated and efficient, and to minimize the accidents due to human errors; however, at the same time, it also allows for the integration of advanced computing in core operations, Internet connection as an integral part, as well as the collection, processing and storage of a wide range of data. The increasing dependencies on ICT systems, Internet connection and data make the maritime transport sector more

---

<sup>334</sup> Kizzi Asala, africanews, 2021, <https://www.africanews.com/2021/01/12/the-gulf-of-guinea-is-a-maritime-battleground-over-oil-wealth/>

<sup>335</sup> Meera Nair, Rutherford, Climate Change and Cyber Security: What to Expect in Financial Services <https://www.rutherfordsearch.com/blog/2021/09/climate-change-and-cyber-security-what-to-expect-in-financial-services>

appealing to cyberattacks and data breaches. Alarmingly, with smart and autonomous maritime transport, cyber risks and threats to the sector will presumably continue to grow in terms of volume, complexity and severity.

Looking at different recent incidents, and listening to ongoing debates about the impact of cyberattacks and data breaches on democracy, although concerns are mainly centered on election manipulation and voting system hacking [Bund 2016], it is evident that cyberattacks can be used to damage the norms and standards of democracy. The EU cybersecurity strategy has emphasized the importance of cybersecurity for democracy in the EU and its Member States [EC 2020A]. In addition to a free and fair electoral process, democracy involves guaranteeing basic rights and civil liberties. These integral components of democracy can be targeted and influenced using cyberattacks and data breaches. Sandoz [Sandoz 2012] itemised a series of harmful activities, including environmental degradation, smuggling, human trafficking, narcotics trafficking, and proliferation of weapons of mass destruction, in which state and non-state actors can engage in the absence of effective maritime security and governance. Many of these could have a prejudicial impact on fundamental rights and democracy.

Connecting maritime transport to the Internet (e.g. smart, and autonomous maritime transport) could attract malicious actors from around the world who want to exploit the vulnerabilities in ships' ICT and Operation Technology (OT) systems with the intent to disturb global trade, food security and tourism (freedom of movement), as well as threaten human life (rights to live). For example, smart and autonomous maritime vessels (with most principles similar to self-driving vehicles) can be vulnerable to hacking [ENISA 2021B] because of the advanced computers they contain and their Internet connection. Malicious actors with access to primarily degree three (remotely controlled) and degree four (fully autonomous) vessels can use them to cause serious damages to property, life and social stability. To get a sense of some potential impacts, let us consider the example of an autonomous ship under the control of hackers or terrorists, and examine how they could take advantage of this situation.

- The hacked ships can be used to obstruct choke points in critical maritime trade routes, delaying the transport of container ships with the intention of disrupting maritime supply chains. With 75% of Europe's external trade moving on the oceans [EC 2019], such cyberattack-induced disruptions could cause serious damage to the economy, as well as related chaos in society.
- Terrorists can use the hacked ships to cause maritime collisions and accidents, or attack coastal infrastructures. Such incidents could cause huge damage to life and property, as well as creating fear among people who regularly travel by ship or live in coastal regions.
- Criminal behaviours and human-induced disasters, such as smuggling of narcotic drugs and weapons of mass destruction, as well as trafficking of illegal immigrants, could potentially increase. There will be nobody in the ships to apprehend, prosecute and punish.

The risk of such malicious activities is not only from non-state actors but also from a rogue state or state-sponsored actors who would use them as cyber warfare tactics or as instruments to pursue geostrategic interests.

The risk to democracy in maritime transport is not only from outsiders but also from the people associated with the sector. Indeed, the maritime transport sector is a major player in the global supply chain, but it is

also a major polluter of water and air.<sup>336</sup> Releasing greenhouse gases and polluting the ocean by maritime transport are some of the highest environmental concerns (seize the right to a clean and healthy environment). Similarly, corrupt staff in the ships might help antisocial elements in their crimes in return for monetary or other types of benefit.

Therefore, the actions taken in relation to maritime transport in the name of business, or whatever else, must not outweigh the current and foreseen fundamental rights of people. Furthermore, there is an imperative need for a more collaborative and global approach to tackle the cybersecurity threats in maritime transport, since the repercussions of a cyberattack may extend beyond national borderlines and jurisdictions.

### **7.6.7 Contributions to the EU CyberSecurity Strategy for the Digital Decade**

EU Directive 2008/114/EC lists maritime infrastructure (both “Inland waterways transport” and “Ocean and short-sea shipping and ports”) as critical, and up to now its dependency on ICT and the Internet has been limited. However, this will change tremendously with MASS in use and so will the need for cybersecurity.

The first dimension (Section 1.1) of “The EU’s Cybersecurity Strategy for the Digital Decade” aims at strengthening the cyber-resilience of critical infrastructures, essential services, as well as democratic processes and institutions. Research on cybersecurity for MASS, especially by adopting a security-by-design approach, will contribute to accomplishing a cyber-resilient MASS system. In addition, this will help to mitigate the several risks to democratic processes arising from the misuse of MASS, described in Section 7.6.7 of this report.

Similarly, the third dimension (Section 3.1) of “The EU’s Cybersecurity Strategy for the Digital Decade” focuses on boosting the EU’s capabilities and leadership by introducing new standards, norms and frameworks. MASS is ongoing research, with current research works primarily focusing on resolving its safety and security risks or concerns. Encouraging more research initiatives in this new and emerging sector is a good and challenging opportunity for the EU and its partners to boost EU capabilities, while also achieving leadership in the sector.

#### **7.6.7.1 Resilient infrastructure and critical services**

The transport sector has been recognized as one of the primary critical infrastructures, at both a European and an international level. Thus, building resilient maritime transport systems will directly contribute to developing resilient critical infrastructures and services. Developing resilient maritime systems has been identified as one of the main research challenges for maritime transport cybersecurity in this roadmap (see Section 7.6.13), and is closely related with other challenges, such as the early identification of emerging threats and risks, hardening of critical maritime systems and the protection of autonomous ships. Therefore, the work on this vertical makes a direct contribution to the EU Strategy for building resilient infrastructures and services.

#### **7.6.7.2 Building a European Cyber Shield**

In an attempt to build a European Cyber Shield, the EU’s cybersecurity strategy [EC 2020A] proposes for initiatives to build a network of Security Operation Centres across the EU, establishing new centres and

---

<sup>336</sup> Financial Times, <https://www.ft.com/content/642b6b62-70ab-11e9-bf5c-6eeb837566c5>

improving existing ones, while training and developing the skills of the people who operate them. This network is important for sustained collaboration and cooperation in cybersecurity, so as to detect potential cyber incidents promptly and issue timely warnings to all related stakeholders, so that the damage can be prevented or minimized. Next, most Member States have made important strides in developing cybersecurity strategies that prioritize their national security and interests. The Directive on Security of Network and Information Systems (NIS Directive) [NIS DIRECTIVE 2016] is an important milestone in the pathway to building a European cyber shield. The NIS Directive strives to achieve a high common level of security of network and information systems within the EU, by means of:

- Improved cybersecurity capabilities at the national level.
- Increased EU-level (cross-border) collaboration and cooperation.
- Risk-management and incident-reporting obligations for operators of essential services and digital service providers (national supervision of critical sectors).

These initiatives to build up resilience in each Member State, extend cooperation within the EU and facilitate capacity building are commendable efforts to enhance awareness of the cyber situation and improve shielding; however, these approaches may not be sufficient to protect the EU region and its Member States from the rapidly changing environment and context of cybersecurity. The European Political Strategy Centre, therefore, has alerted the EU and its Member States to anticipate unimaginable scenarios, in the worst case advising them to be ready to counteract even cyber warfare (which could fall within the remit of Article 5 of the NATO Treaty), or cyberattacks carried out in the pursuit of geostrategic interests. In addition, the centre recommends that the EU should assign priority to the following:

- Building up Europe's cyber capabilities to detect, prevent and control rapidly emerging and evolving (in environment, context and sophistication) cyberattacks from non-state and state-sponsored actors.
- Building a cybersecurity mind-set in different stakeholders (businesses, public organizations, law enforcement authorities, and individuals) in the Union and its Member States. They should be aware of the security risks and threats to which they are exposed and vulnerable and, accordingly, be prepared with both technical and non-technical countermeasures. All stakeholders should promptly report any cyber incident to the competent authorities.
- Developing the cybersecurity skillsets of European citizens. In addition, taking actions towards updating and retaining highly skilled people. For example, the drifting of staff from regional and national agencies to private companies, and from the EU to foreign countries must be prevented.
- Eliminating excessive dependencies on externally developed cybersecurity technologies, including hardware and software. The EU and its Member States should attract more investment in cybersecurity through business-friendly policies and a competitive environment (e.g. economic competitiveness).
- Maximizing institutional collaboration and cooperation on cybersecurity in the EU, which could lead to the establishment of a European Coordination Platform for cybersecurity. The responsibilities of this platform could be detection, prevention, cooperation, protection and prosecution. This will require relevant public policies, backed up with appropriate resources to implement them.

- Having joint European risk strategies and coordinated political responses against large-scale attacks.
- Investigating and establishing suitable forms of collaboration with industry and civil society, as well as with like-minded third countries, to close the loopholes in Europe's cyber shield.

The EU approach for a cyber shield is primarily defensive. Looking at the current scenarios in cyberattacks, it is possible that the reactive approach is not enough, and the EU may feel a need for an offensive cyber capability. The EU and its Member States should therefore consider the offensive approach as an option for which it should be prepared.

In order to achieve a European cyber shield, every sector that is reliant on network and information systems, including Maritime Transport, must also be resilient to attacks. The EU Maritime Security Strategy (EUMSS) Action Plan 2020 includes cyber and hybrid threats as an integral part [EC 2020B]. It addresses the following key areas: international cooperation, capability development, research and innovation, and education and training. Its Action No. A.3.8. emphasizes the need to: “[i]mprove the integration of a cybersecurity dimension in the maritime domain in terms of capabilities, research and technology, and industry, building on civil-military coordination and synergies with EU cyber policies related to both cybersecurity and cyber defence, in line with the NIS Directive and international recommendations and regulations such as SOLAS XI-2 and the ISPS Code and their future updates. This will include the exchange of best practices and development of joint projects by the EU Member States on maritime cyber-attack prevention.” [EC 2020B] The components incorporated in the Action Plan are the same that are necessary for a European cyber shield and so should be applicable to a maritime transport cyber shield. However, the case of maritime transport involves not just one sector, but includes many other sectors on which it depends for smooth (safe and secure) operation or functioning. These dependencies should also be resilient for a maritime transport cyber shield. Moreover, along with organisations such as the European Maritime Safety Agency (EMSA),<sup>337</sup> the sector also needs to cooperate with various European agencies for cybersecurity.

#### **7.6.7.3 An ultra-secure communication infrastructure**

In the context of the maritime transport cybersecurity roadmap, securing maritime communication systems has been recognized as an important research challenge. As maritime communication systems involve various types of communication system, including landline (for shore systems), wireless and satellite communications, developing secure maritime communications will contribute to, and at the same time will benefit from, research efforts for ultra-secure communication infrastructures. Admittedly, however, as the maritime industry works on a low profit margin, developing ultra-secure maritime communication infrastructures that may require high costs (e.g. quantum communications) will not be a primary goal for this sector.

#### **7.6.7.4 Securing the next generation of broadband mobile networks**

Network access becomes more ubiquitous through the years. We expect that mobile networks will be expanded, and even critical infrastructures that used to be isolated will be part of the same network. In that sense, we are progressing towards a unified borderless network, which brings convenience—everybody has

---

<sup>337</sup> EMSA, <http://www.emsa.europa.eu/about.html>

access to the Internet from everywhere—while increasing the risk of cyberattacks that use the network to access remote targets.

In this vertical, we have applied secure communications to a relatively untouched domain: communication between maritime vessels and landline devices. We expect that similar cases, where a remote critical infrastructure needs to be connected securely with other typical systems, will appear in other domains, apart from maritime transport. Our developments in this vertical may, therefore, find applications in similar setups that are not directly related to maritime activities, but involve parts of a generic secure broadband network that is accessible to all.

#### **7.6.7.5 An Internet of Secure Things**

Various IoT technologies are also applied in the maritime transport, including proximity sensors, collision avoidance systems, RFID and other cargo tracking technologies, to name just a few. As the integration of IoT technologies increases the connectivity and interaction between systems, it also leads to increased exposure to threats and to extended attack paths. When IoT technologies are integrated in critical cyber-physical systems, as is the case in the maritime transport sector, emphasis should be placed on IoT security. Extensive security testing and validation will be required for IoT technologies deployed in maritime systems. Towards this direction, there is a need for legal and regulatory initiatives that will enforce the development, testing and validation of secure IoT technologies, for both the manufacturers and the operators, when IoT technologies are applied in critical infrastructures and systems.

#### **7.6.7.6 Greater global Internet security**

The EU's Cybersecurity Strategy for the Digital Decade 2020 [EC 2020A] has set forth primarily three major measures for greater global Internet security, as follows:

1. To ensure the integrity and availability of the global DNS root system. In order to achieve that, the plan is to:
  - a. Assess the role of the two EU DNS root server operators in guaranteeing that the Internet remains globally accessible in all circumstances.
  - b. Encourage all relevant stakeholders, including EU companies, Internet Service Providers (ISPs) and browser vendors, to adopt a DNS resolution diversification strategy.
  - c. Support the development of a public European DNS resolver service that will be transparent, and will conform to the latest security, data protection and privacy requirements by design, following default standards and rules.
2. To accelerate the uptake of key Internet standards, including IPv6 and well-established Internet security standards and good practices for DNS, routing, and email security, not excluding regulatory measures, such as a European sunset clause for IPv4 in the EU Member States and partner countries.
3. To work on mechanisms for more systematic monitoring and gathering of aggregated data on Internet traffic and for advising on potential disruptions.

In addition to the above, Sherman [Sherman 2020] has suggested investing in cyber diplomacy to advocate for norms of non-interference with core Internet protocols at the global level. Similarly, Purdy [Purdy 2021] has advocated for a “Zero trust” policy, which means that no untested technology should ever be trusted.

The maritime transport sector is not directly connected to the greater global Internet security. However, the sector can still indirectly contribute to the objective to an extent; for example, by:

- Using services only from ISPs and browser vendors that have adopted a DNS resolution diversification strategy.
- Promptly adopting well-established standards and protocols, for example, IPv6.

Adopting Internet products and services only after they have been thoroughly tested (for conformance to relevant standards and practices).

#### **7.6.7.7 A reinforced presence on the technology supply chain**

5G connectivity in autonomous ships is an ongoing and long-term cybersecurity research challenge in the maritime transport sector (see section 7.6.15). The EU could invest in associated innovators to promote solutions for securing 5G maritime transport networks by expanding the research into secure communication technologies. In relation to the NIS 2 Directive proposal, maritime transport CIs are associated with a variety of entities that operate essential services for the EU economy. In this vein, the EU could invite industry and research communities from the maritime transport sector, in collaboration with cybersecurity domain expertise from member states, to gather important knowledge on secure sensitive infrastructures, such as maritime transport systems that rely on IT technologies and automation, and thereby reinforce the EU's digital sovereignty.

#### **7.6.7.8 A Cyber-skilled EU workforce**

As presented in section 7.1, maritime transport is a complex sector, interacting with a range of industries (e.g. energy, logistics, manufacturing, etc.). To implement its complex services, it operates a variety of different and heterogeneous interconnected cyber and physical infrastructures (e.g. SCADA systems, such as LNG tanks controlled by LNG monitoring systems, including Programming Logic Controllers that use Modbus protocols) that create strong cyber and physical interdependencies with extensive cascading effects in the event of a cyberattack on such systems. For instance, a cyberattack on the LNG monitoring system could cause damage to the interconnected LNG tank.

In addition, there is a trend to increase the use of emerging technologies in the maritime transport CIs, such as AI-enabled technologies, Cloud and Edge Computing, e.g. to facilitate maritime logistics operations for the collection, transport and transmission of data retrieved from sensors, cameras and other information-gathering and data capturing devices.<sup>338</sup> For instance, machine learning algorithms used for remote monitoring—e.g. in Automatic Identification Systems (AIS), to increase accuracy in the forecasting of traffic density or quantum technology—will be adopted in the coming years for next-generation container ships. Section 7.6.2.4 of the current vertical describes how the utilization of emerging technologies in these complex interrelated maritime transport CIs could generate new emerging threats, as such technologies are still a new area of investigation that could involve cascading effects.

---

<sup>338</sup> PierNext, Port de Barcelona, <https://piernext.portdebarcelona.cat/en/logistics/machine-learning-applied-to-the-maritime-sector-navigating-a-sea-of-data/>

In this context, creating EU synergies with entities from the maritime transport industry domain and investing in further investigation of the heterogeneity and complexity of maritime transport CIs, with their technical specificities and security peculiarities that can highly impact a range of industries, can reinforce EU strategic initiatives in the form of regulatory measures for a more secure Internet and connectivity of maritime transport CIs, reinforcing security in the communication of infrastructures that harness AI-enabled and quantum-based technologies. Promoting such strategies could leverage the EU cyber-skilled workforce.

#### **7.6.7.9 EU leadership on standards, norms and frameworks in cyberspace**

Maritime governance is fragmented at several levels, international, regional and national. Every major country wants to lead the race to set up relevant standards and norms, or to come up with appropriate frameworks, either working in isolation or in partnership with other countries. In the context of maritime transport, the EU has taken some major steps to get ahead in this race. They are:

- General Data Protection Regulation (GDPR).<sup>339</sup> This helps to address the data protection and privacy issues from data exchange that will occur between Member States and other countries within the context of maritime transport.
- NIS Directive on Security of Network and Information Systems [NIS DIRECTIVE 2016]. The three parts of the directive (i.e. national capabilities, cross-border collaboration, and national supervision of critical sectors, including maritime) help to address several concerns emerging from the use of network and information systems in maritime transport. Their relevancy will grow with smart and autonomous ships.
- ENISA Guidelines for Navigating Cyber Risk [ENISA 2020E]. The guidelines provide port operators with a set of good practices to help them identify and evaluate cyber risks, and effectively identify suitable security measures.
- EU Guidelines for safe, secure, and sustainable MASS trials.<sup>340</sup> The guidelines pave the way for MASS trials in safe, secure, and sustainable ways. In addition, they provide guidance for risk assessments.
- The EU's Maritime Security Strategy (EUMSS) [EC 2020B] Action Plan. The action plan covers overall maritime security, with a view to protecting the strategic maritime interests of the EU worldwide. It has cybersecurity as an important item on the plan's agenda.

#### **7.6.7.10 Cooperation with partners and the multi-stakeholder community**

As maritime transport services require the interaction of systems operated by various partners and stakeholders (e.g. port authorities, customs, shipping companies, logistics, etc.), securing maritime transport systems requires the cooperation of the involved stakeholders and business partners. Towards this direction, in this roadmap we have identified research challenges that strongly depend on such cooperation. For example, maritime-specific threat modelling and risk assessment methodologies require the development of

---

<sup>339</sup> GDPR, <https://gdpr-info.eu/>

<sup>340</sup> EC1, [https://transport.ec.europa.eu/news/european-commission-encourages-maritime-future-which-includes-autonomous-and-sustainable-ships\\_en](https://transport.ec.europa.eu/news/european-commission-encourages-maritime-future-which-includes-autonomous-and-sustainable-ships_en)

tools that support the collaborative identification and modelling of threats and risks by multiple maritime business partners, as these threats/risks may cascade among systems operated by different stakeholders.

#### **7.6.7.11 Strengthening global capacities to increase global resilience**

As described in previous related sections (7.6.1.6 and 7.6.8.1), the maritime transport sector is considered to operate primary critical infrastructures (CIs), at both European and international level. At the European level, this is supported by the EU 2 DIRECTIVE proposal [NIS 2 DIRECTIVE proposal 2020], where CI operators of maritime transport (i.e. port-related operators, operators of inland, sea and coastal passenger and freight water transport, etc.) are considered “Operators of Essential Services”.

Joint collaborations among international entities to strengthen maritime transport CIs resilience can affect the cyber resilience capacity positively on a global scale, as maritime transport is a key enabler of the global economy. This is justified, knowing that maritime transport CIs are highly connected with CIs of many other industries (e.g. vehicles industry, energy, logistics, etc.) and that approximately 80% of the volume of international trade in goods is carried by sea (the percentage is even higher for most developing countries), while over 70% by value is carried by sea and is handled by ports worldwide.<sup>341</sup> Thus, tackling cybercrime and addressing cyber threats in the maritime transport environment can reinforce the digital economy globally. On this basis, investing in resilient maritime systems has been recognised as one of the main research challenges for maritime transport cybersecurity in the current roadmap (see Section 7.6.13).

According to [Tafazzoli 2019] maintaining the sustainability of CIs involves the following main measures: (1) minimising the adverse impacts of the infrastructure on people through maintenance; (2) keeping the maintenance operations sustainable; (3) sustainable allocation of material to the maintenance process; and (4) environmental protection and restoration in maintenance operations.

There are global maritime institutions and policy makers that contribute with good practices, guidelines and statistical reports to leverage knowledge about countering cyber threats and reinforcing the resilience of maritime transport CIs. Indicatively, these include: the specialised United Nations agency “International Maritime Organization” (IMO), which aims to improve the sustainability of maritime transport CIs; the International Association for Classification Societies (IACS), which has made a unique contribution to maritime safety and regulation through technical support; the United Nations Conference on Trade and Development (UNCTAD), which sets sustainable development goals; the international shipping association Baltic and International Maritime Council (BIMCO); the International Association of Independent Tanker Owners (INTERTANKO); the World Shipping Council, which supports the security of the shipping industry; and the global trade association of the International Chamber of Shipping. The EU, as a means of supporting efforts to construct external cyber-capacity, could encourage synergies with such international specialized organisations and agencies to exchange relevant knowledge and promote the importance assigned to maritime cybersecurity legislation, policy and certification. This could boost the cybersecurity resilience of maritime CIs and strengthen cybersecurity in the face of rapid digital development.

---

<sup>341</sup> UNCTAD, <https://unctad.org/topic/transport-and-trade-logistics/review-of-maritime-transport>

### 7.6.8 Sector-specific Dimensions

Maritime transport has been a catalyst for the EU economy over its history, driving a leading role in freight trade and being a vital source of its employment and income [ENISA 2011; ENISA 2020E]. It is a multi-compound industry sector, which overall performance enfolds a conflation of other Industries (i.e. logistics, warehouse management, automobile, energy, geospatial, finance, waste management, LNG, etc) utilizing both obsolete technologies (i.e. analog transponders, radio telex, telegraphy etc) and modern and emerging technologies (blockchain-based logistics, Distributed Ledger Technology (DLT) for shipping operations, IoT-based ship berthing, augmented reality for unmanned vessels, integrated renewable energy systems, 5G connectivity for maritime communication, etc).

A crucial part of this sector is that is capable of operating through the remote collaboration of heterogeneous dispersed nodes (i.e. autonomous navigation of vessels, Remote Terminal Units (RTUs) that monitor gantry cranes and forklifts while stevedoring, satellite communication to transmit signals for vessel-to-port and port-to-vessel communications. In the modern digital era, such highly interactive distributed infrastructures (i.e. SCADA, AIS, ICTs, etc) are cyberphysical-dependent (i.e. CCTV cameras rely their backup storage on a CCTV database System (OS), a centrifugal pump is controlled by a fuel monitoring system, etc). The dispersed connectivity among maritime transport infrastructures, increases cyber adversaries' appetite to attack on critical parts of the system and produce asset damage (i.e. CCTV monitor off), service disruption (i.e. AIS system crash) even loss of human life and environmental harm (oil tanker explosion in ocean waters could kill vessel employees and cause severe sea pollution). As a result, a cyber-attack on such infrastructures can have a devastating impact to the maritime ecosystem. In addition, as the maritime transport sector is directly connected with other verticals (i.e. incident reporting, supply chain security, identity management and smart cities) a sophisticated multi-vector cyber-attack can affect and other industries as well (i.e. a daily closure of a vehicle port terminal due to a ransomware attack can have a tremendous financial impact for an automobile industry). Because of this special linkage of the maritime transport with other markets, the preservation of security and resilience of its infrastructure keeping its confidentiality, integrity and availability is a burning issue that needs to be ensured.

In this line, EU has set on top of priorities to keep the maintenance of secure long-term performance of the maritime transport system as a whole. The maritime governance needs clarification of roles and responsibilities at EU level to address cybersecurity open issues [ENISA 2011]. The provision of such recommendations could tailor the estimation of the budget required to invest on cybersecurity initiations that expand the security awareness borders and enable to better foresee a realistic expected outcome in a maritime stakeholders' collaborative environment [ENISA 2011]. To leverage security measures that could practically address the identified threats (described in section 7.4) and build a strong cybersecurity competence network in the maritime transport sector, the technical specificities and particularities of the critical maritime transport infrastructures along with their asset interdependencies should be taken into account on organizational, sectorial and cross-sectorial level scrutinizing the inherent processes, the key-players and the involved assets at service level (ENISA 2020E; KAPP 2018) that drive the sector's performance.

## 7.6.9 Summary of the dimensions and impact on the Roadmap

In order to provide a roadmap that is capable of addressing the identified cybersecurity challenges of the current vertical efficiently and in a timely manner, a thorough analysis of maritime transport has been conducted, exploring its different cybersecurity aspects. To this end, maritime transport has been analysed in terms of its CIs and critical services (section 7.3), the emerging cyber threat landscape of the domain, and the major threat actors (section 7.4) and notable domain security incidents (sections 7.4 and 7.5).

To identify the cybersecurity research challenges of the vertical, a state-of-the-art analysis was presented (section 7.6.1) to capture information about existing solutions and regulations and recognise domain security gaps. Then, a SWOT analysis was carried out to further investigate the strengths, weaknesses, opportunities and threats related to maritime transport cybersecurity and ensure that the established roadmap will be able to respond properly to the identified cybersecurity challenges (sections 7.6.11-7.6.15) in the short, mid and long terms. An additional analysis of the vertical was undertaken to investigate the role of maritime transport cybersecurity in the context of the most important EU trends where it may be applicable: whether it can reinforce digital sovereignty, affect COVID-19 and public health, influence climate change, or impact fundamental rights and democracy (sections 7.6.3-7.6.7 respectively). Moreover, the cybersecurity views of this vertical were further scrutinized under the scope of the EU Cybersecurity Strategy (section 7.6.8), to determine how to promote the cyber resilience of maritime transport CIs and the continuity of essential services operations, and how to boost EU capabilities and leadership by introducing new standards, norms and practices.

Taking into account the information gathered from these different dimensions, we laid out a *short-term plan* targeted at the *enhancement of attack path discovery algorithms with machine learning techniques* to deliver more accurate results regarding cascading effects and risk propagation during risk assessment, and the *improvement of the capacity of the implemented security controls associated with software hardening*. As regards maritime system communications, *the environmental limitations of the maritime transport sector, such as network availability and communication costs, have been set up and validated* to address current challenges and *develop VDES-ready solutions that could support both satellite and radio communication*.

## 7.6.10 Challenge 1: Early identification and assessment of risks, threats and attack paths for critical maritime systems

A basic challenge that the maritime sector faces because of its dynamic environment is the early identification of novel, hidden or underestimated risks and threats. With the introduction of state-of-the-art equipment – which includes communication devices, interconnected systems and other cyber-physical systems, working together under a broad structure – a vast range of previously unidentified vulnerabilities and attack paths occurs. Those threats can be utilized by adversaries to impact assets and services that are critical to maritime organizations. The NotPetya attack described above is a good example of the impact of such hidden/underestimated attack incidents. If that attack path had been identified in time, the company would have avoided a 300-million-dollar hit. Hence, the early identification of such threats is a matter that actively affects maritime organizations and companies.

### Specific Research goals:

- Design and implement efficient cyber-attack path discovery algorithms, with the support of advanced and innovative techniques. Such algorithms require a sequence of steps in order to provide

effective vulnerability identification on an information system. Throughout those steps, various methodologies and tools are utilized to identify and assess hidden and underestimated risks deriving from cascading threats and complex attack paths. The integration of novel machine learning techniques may assist in the identification and assessment of the cascading attack paths.

- Design evidence-based and scenario-based risk assessment approaches, based on recent cybersecurity incidents that entailed sophisticated attacks and on scenarios created to support active learning processes, such as problem-based and case-based learning.
- Develop ways to procure stable datasets, based on existing threat/risk characteristics catalogued in public repositories. Using those datasets, neural networks can be trained to predict vulnerable attack paths by identifying a set of characteristics when scanning new systems.
- Develop ways to visualize the vulnerable attack paths and the flow of the possible attacks. List the vulnerabilities and attack patterns identified in this process to provide automated attack reports.

#### **JRC Cybersecurity Domain:**

- Security management and governance
  - Risk management including modelling, assessment, analysis and mitigation
  - Modelling of threats and vulnerabilities
  - Attack modelling, techniques, and countermeasures
  - Privacy impact assessment and risk management
  - Standards for information security
  - Attack modelling, techniques, and countermeasures

#### **JRC Sectorial Dimensions:**

- Transportation
- Manufacturing and supply chain
- Telecom digital infrastructure

#### **JRC Technologies and Use Cases Dimensions:**

- Information systems
- Critical infrastructures
- Artificial intelligence
- Hardware technology
- Human machine interface

### **7.6.11 Challenge 2: Security hardening of maritime infrastructures, including cyber and physical systems**

In maritime transport, the use of legacy systems is common. For instance, vessels or port authorities heavily rely on embedded systems that are highly customized and hard to update. Additionally, it is not trivial to migrate such systems to new programming languages/systems that do not suffer from memory corruption vulnerabilities. Protecting these systems is challenging because of (a) deep esoteric/custom designs, (b) a lack of open standards, (c) difficulties in auto patching/updating. Not protecting such systems may have several serious consequences.

#### **Specific Research Goals:**

- **Analyse software and identify unsafe components.** In the maritime sector, highly customized software may be used. The attribution of such software may be difficult in many cases. Such attribution involves, for instance, identifying the programming system used to implement a particular program, possible compiler options used that enable security mitigations, or the existence of a run-time environment that offers additional security. Analysis of unknown, non-standard, software for such properties can be challenging. Current analysis tools should be enhanced in order to perform such tasks.
- **Harden programs with no recompilation.** Programs written in unsafe programming systems may contain memory vulnerabilities, which can be devastating for the security of systems (e.g. WannaCry, Petya/NotPetya). Usually, protecting such programs is based on changing the source code. Unfortunately, in the maritime sector, it is very likely that source code of existing software is not available. For such cases, protecting binary-only programs must be explored.
- **Harden programs without modifications.** Protecting binary-only programs is fairly challenging; nevertheless, there are cases when highly customized and exotic software may be hard to rewrite. In such cases, protecting the software cannot be done by using binary rewriting. Techniques that are entirely program-agnostic, such as pre-loading the binary with secure memory allocators can be of use.

#### JRC Cybersecurity Domain:

- Software and hardware security engineering

#### JRC Sectorial Dimensions:

- Transportation
- Manufacturing and supply chain
- Telecom digital infrastructure

#### JRC Technologies and Use Cases Dimensions:

- Critical infrastructures
- Hardware technology
- Industrial IoT and Control Systems
- Information systems
- Internet of Things, embedded systems, pervasive systems
- Operating systems

### 7.6.12 Challenge 3: Resilience of critical maritime systems

A major challenge is assuring the resilience of critical maritime systems. Ideally, critical maritime systems should continue to provide a minimum service level during or after a cyber and/or combined cyber-physical threat, and they should quickly adapt and recover from such unwanted events.

#### Specific Research Goals:

- **Ensuring the robustness of the maritime ICT infrastructures against cyber-attacks.** This research goal involves the development of novel architectures and algorithms that will enable maritime systems to withstand unwanted events, such as deliberate attacks, accidents, or naturally occurring threats, without exhibiting complete failure of critical operations. System hardening may also assist towards this direction.
- **Ability to quickly adapt to security threats.** This research goal entails the development and implementation of monitoring techniques supported by AI algorithms that will analyse the threat events and will enable systems to quickly adapt to attacks and apply proper mitigation controls. In

addition, novel methodologies and tools need to be developed to allow the fast recovery of critical maritime systems, such as those used in autonomous ships.

#### **JRC Cybersecurity Domain:**

- Operational incident handling and digital forensics

#### **JRC Sectorial Dimensions:**

- Transportation
- Telecomm digital infrastructure

#### **JRC Technologies and Use Cases Dimensions:**

- Critical infrastructures
- Satellite systems and applications
- Internet of things, embedded systems, pervasive system
- Operating systems
- Hardware technology
- Human machine interface
- Big data
- Cloud, Edge and Virtualization

### **7.6.13 Challenge 4: Maritime system communication security**

A challenge that is related to many threats in the maritime industry is the creation of secure and stable communication channels. Many incidents in this sector have been connected with traffic interception attacks, GPS spoofing attacks and other attacks that meddled with communication methods. Therefore, it is required that maritime companies implement multiple communication methods on their fleets, in order to enable the verification of the apprehended information by a second source, and in order to create availability (e.g. satellite communication for dead zones). While the newly developed VHF Data Exchange System (VDES) specification, which will enable data transmissions between ship-to-ship and ship-to-shore, is about to become an ITU<sup>342</sup> standard, work still remains to be done to protect the application data that is being transferred over this communication channel.

#### **Specific Research Goals**

- ***Develop wireless access control mechanisms through secure channels, to be utilized in cases where remote intervention is required on vessels.*** As the possibility for remote intervention is a clear function requirement, wireless access control mechanisms based on secure channels are a necessity, in order to enable such functionality.
- ***Design and develop trust infrastructures that take into consideration the environmental limitations of the maritime transport sector, such as the network availability and the communication costs.*** Since stability of communication is an issue, it is crucial to facilitate the availability and stability of the communication solutions. As such, the solutions need to be scalable and redundant.

---

<sup>342</sup> ITU stands for International Telecommunication Union.

- ***Design and implementation of maritime systems that utilize both satellite and radio communication means.*** Given the need for stability and redundancy, this goal addresses a part of the solution towards achieving network availability.
- ***Design and demonstrate a trust infrastructure that facilitates preservation of integrity and confidentiality aspects associated with maritime communication.*** As the common incidents in maritime sector are associated with interception attacks, it is crucial to have solutions that support the communication not being exposed to intruders and not being compromised.

#### **JRC Cybersecurity Domain**

- Network and distributed systems

#### **JRC Sectorial Dimensions**

- Transportation
- Telecomm digital infrastructure
- Space

#### **JRC Applications and technologies**

- Critical infrastructures
- Satellite systems and applications

### **7.6.14 Challenge 5: Securing autonomous ships**

Because the ICT system architecture and operations of autonomous ships have not been fully specified, multiple cyber security issues remain open and should be addressed. The overarching challenge towards this direction is the identification and development of tools for the management and mitigation of combined safety and security risks, especially given the nature of such systems where, ICT plays a primary role in safety critical operations. Additional challenges arise in the specification of the security architecture and services required to be deployed, not only on board the maritime autonomous surface ships, but also across the remote-control centres that may coordinate their operations, with special focus on the corresponding communication architectures. Additionally, a fundamental requirement arises with respect to the development and deployment of suitable integrated security, safety and ship management system (IS3MS) that can support and protect operations across the distinct autonomy levels.

#### **Specific Research Goals**

- ***Comprehensive communication architecture for autonomous ships.*** With the introduction of autonomous ships, maritime communication is required to cope with the new communication and security requirements. New entities are added to the maritime context, such as the remote-control centre and advanced new ships. Additionally, more data is generated and is expected to be transferred from the ship to the remote-control centre with different communication requirements. A main research focus in future maritime communication architecture should be on ship-to-ship communication, which can provide some features to ships that have limited access to the internet. Some studies have proposed the concept of delay tolerant networks (DTN) in the maritime sector, as a possible solution to certain connectivity issues related to coverage. DTN can be used to improve the routing schemes for the traffic, so as to achieve better end-to-end packet delivery [LGP+ 2010] [LDC 2013]. Notably, not much work has been presented that discussed communication security for autonomous ships. Therefore, an architecture that adopts security by design is needed.
- ***5G and satellite integration for ship connectivity in autonomous ships.*** To solve the issue of limited bandwidth, the current direction is toward 5G. Several works have identified 5G as a

possible solution to several connectivity issues in maritime communication. The notion of heterogeneous communication in 5G that includes satellite communication integration would aid in solving many connectivity issues for autonomous ships [HHKSR 2017] [HOM+ 2017].

- ***Unified security and safety risk management of heterogeneous components in autonomous ships.*** Utilizing software-defined networks (SDN) and network function virtualization (NFV) is one proposed direction to unify the application of security functions in a heterogeneous network of systems on board ships [FSS+ 2017]. SDN and NFV can be leveraged to add security properties to such networks.
- ***Global navigation satellite system (GNSS) security.*** GNSS is crucial for several autonomous ship functions, such as navigation and search and rescue. With GNSS being a single point of failure that is vulnerable to several attacks, such as spoofing and jamming, an active research direction is GNSS signal authentication, resiliency, and integrity.

### JRC Cybersecurity Domains

- Security management and governance
  - Risk management, including modelling, assessment, analysis and mitigation;
  - Continuous monitoring;
  - Threats and vulnerabilities modelling;
  - Attack modelling and countermeasures;
- Network and distributed systems
  - Network security (principles, methods, protocols, algorithms and technologies);
  - Distributed systems security;
  - Telecommunications network security;
  - Network attack propagation analysis;
  - Fault tolerant models;
- Software and hardware security engineering
  - Security and risk analysis of components compositions;
  - Vulnerability discovery and penetration testing;
  - Intrusion detection and honeypots;
- Operational incident handling and digital forensics
  - Incident analysis, communication, documentation, forecasting (intelligence based), response;
  - Vulnerability analysis and response;
  - Resilience aspects;
- Human aspects
  - Human-related risks/threats (social engineering, insider misuse, etc.);
  - Automating security functionality;
- Cryptology (cryptography and cryptanalysis)
  - Message authentication;
- Data security and privacy
  - Design, implementation, and operation of data management systems that include security and privacy functions;

### JRC Sectorial Dimensions

- Transportation
- Telecomm digital infrastructure

### **JRC Applications and technologies**

- Critical infrastructures
- Satellite systems and applications
- Robotics
- Hardware technology
- Cloud, edge and virtualization
- Artificial intelligence
- Big data

## **7.7 Mapping of the Challenges to the Big Picture**

The dynamic environment of the maritime transport sector incorporates a bundle of complex, interdependent and interconnected systems and services. Considering this, and in accordance with the emerging cyber threat landscape against the maritime transport infrastructures, there is a compelling need for early identification and assessment of risks, threats and attack paths for these critical maritime systems (challenge 1). The means of communication supporting these multiplex networks (i.e. VDES communication satellite connectivity, etc.) exhibit different specificities as regards their IT infrastructure resulting in different security requirements. Bearing in mind the inherent economic constraints in enterprises towards covering such composite security requirements of their infrastructures, the creation of secure and stable communication channels is a demanding challenge. In this vein, there is an open space for research to investigate methods that can provide sufficient maritime communication security creating a circle of trust (undertaking cryptographic measures) among the maritime community (challenge 4).

Another issue in the maritime transport environment, is that the operating critical infrastructures present backward compatibility (i.e. they incorporate obsolete software making hard to update) engaging considerable flaws. Implementing security hardening on such maritime transport cyber-physical systems is urgently needed to reduce bugs and strengthen their integrity (challenge 2). Taking into account all the above requirements, the concern of improving the maritime infrastructures' preparedness against unwanted events, preserving the security and providing trustworthiness must be effectively addressed in terms of ensuring the infrastructures' robustness and their quick adaptation to security threats and thus to pursue the resilience of the critical maritime systems (challenge 3). Eventually, the consolidation of advanced technology in the maritime sector has initiated new technical features in transportation, such as the presence of autonomous ships. In this light, the unification of security, risk management and trustworthiness in the maritime sector should be considered in the context of building comprehensive navigation and communication architectures with advanced security features to provide safety in the autonomous ships and secure their connectivity (challenge 5).

## **7.8 Methods, Mechanisms, and Tools**

### **7.8.1 Risk management and threat modelling methodologies for the Maritime Transport sector**

The main goal of risk management is (in general) to protect business assets and minimize costs in case of failures; it thus represents a core duty of successful company management. Hence, risk management describes a key tool for the security within organizations and it is essentially based on the experience and knowledge of best-practice methods. These methods consist of an estimation of the risk situation, based on

the business process models and the infrastructure within the organization. In this context, these models support the identification of potential risks and the development of appropriate protective measures. The major focus is on companies and the identification, analysis and evaluation of threats to the respective corporate values. The outcome of a risk analysis is in most cases a list of risks or threats to a system, together with the corresponding probabilities. For risk management in the maritime sector, huge emphasis is placed on physical and object security. In particular, the International Ship and Port Facility Security (ISPS) Code [IMO04] (as well as the respective EU regulation [EC725/2004]) defines a set of measures to enhance the security of port facilities and ships. Therein, methodologies to perform security assessments and to detect security threats are described and a guideline for the implementation of the respective security measures is given:

- Methodologies from the tactical to the strategic level to maximize the effectiveness of assessment for decision making.
- Development of innovative decision support systems for maritime security, involving different communities; integrating of decision support tools in operational environments (i.e. in legacy systems); research efforts in artificial intelligence applicable to security decision support systems.
- Wargames methodologies supported by tools to test scenarios and conflict situations to support the decision making process in the maritime domain.
- Adaptive and dynamic threat modelling and risk assessment methodologies specifically tailored to the needs of the transport sector.

Risk management methodologies can support the early identification and detection of risks and threats. Security tools that can be used from the CyberSec4Europe WP3 portfolio include MITIGATE, CORAS and BowTie Plus. An enhancement of the above methodologies could be the application of threat intelligence knowledge aiming to eliminate the gap between advanced attacks and means of the organization's defences by exploring features of the attack. Currently, there is no collaborative framework to securely exchange and share sensitive data and threat-related information to keep enterprises and key players up to date. In order to implement threat intelligence and information sharing, a framework needs to be invented that has the ability to securely exchange and share sensitive data and threat-related information to keep enterprises and key players up to date. Such a framework would deal with some of the challenges set out in Section 7.7.

### 7.8.2 Secure Autonomous Ships

Since autonomous ships are a relatively recent technological challenge, “off-the-shelf” tools and methodologies for securing maritime autonomous surface ships (MASS) are not very common. In some cases, general-purpose security tools have been fine-tuned for MASS. For example, Kavalieratos et al. have studied and evaluated the utilization of Microsoft's STRIDE methodology [MICROSOFT 2009] for the modelling of threats against MASS.

Leading maritime manufacturers and operators utilize recent developments in ICT towards developing ships with enhanced monitoring, communication and control capabilities, which are referred to as “cyber-enabled”. These include ships that can be controlled from a distance and fully autonomous ships [Loyds 2016]. Ship manufacturers have already designed ships with minimal or even no crew, which can be controlled remotely and are expected to travel the open seas by 2035 [RR 2016]. Most of the remotely operated or fully autonomous ships of the future integrate cyber-physical systems, in which the physical process is controlled by computer-based systems. The interconnections and interdependencies within such a system-of-systems operational environment, integrating ships, links, remote control and service provisioning centres, are still under investigation, with the research domain gaining increasing traction [KKG 2018]. Given the increased interest in automating functions of the shipping industry, classification societies, academia and regulatory bodies have defined appropriate classifications for the autonomy levels

(AL). In particular, Lloyd’s Register proposed seven levels of autonomy for the cyber enabled ship. These are: (i) Manual, (ii) On-ship decision support, (iii) On- and off-ship decision support, (iv) Active human in the loop, (v) Human in the loop – as operator or supervisor, (vi) Fully autonomous rarely supervised, and (vii) Fully autonomous without any human interaction. Furthermore, the International Maritime Organization (IMO) in [RNH 2018] defined four autonomy levels for autonomous ships, namely: 1) AL0: Ship with automated processes and decision support, 2) AL1: Remotely controlled ship (with seafarers on board), 3) AL2: Remotely controlled ship (without seafarers on board), and 4) AL3: Fully autonomous ship. Kavallieratos et al. identified the systems and sub-systems of the cyber-enabled ship, considering the MUNIN project (Unmanned Navigation through Intelligence in Networks) [MUNIN 2016] and the BIMCO report “The Guidelines of Cyber Security Onboard Ships”[RJ 2016].

At this stage, remotely controlled and fully autonomous ships are the priority of most ongoing investigations into autonomous ships. These investigations focus primarily on resolving the challenges that could emerge from the integration of ICT and OT with ship equipment. Safety and security are the two main concerns that are aggressively being investigated. The high dependency on ICT and automated OT, and increased interconnectivity between the ship and onshore infrastructure will also increase potential cyberattacks on autonomous ships. For example, the navigation and control systems of autonomous ships have many similarities to those of autonomous cars, and ENISA [ENISA 2021B] has found that autonomous cars are highly vulnerable to a wide range of attacks. It is, therefore, of paramount importance to properly manage the potential risks and threats as the related technologies continue to advance.

To tackle growing concerns about safety and security threats in autonomous ships, the European Commission, together with EU Member States and Norway, and with input from industry, has developed and issued guidelines for safe, secure, and sustainable trials of MASS [EC 2020C]. The EC guidelines intend to provide guidance on factors to consider in the assessment of MASS trials, including risk assessment. Since MASS is an ongoing project with very limited information available, the guidelines are only preliminary and will be reviewed, updated, and adjusted as more experience is gained with MASS trials conducted according to these guidelines and the results become available, providing more insights into the technology and the procedures used. Similarly, the IMO has issued Interim Guidelines for MASS trials [IMO 2019] and has approved the results of the regulatory Scoping Exercise for the use of MASS [IMO 2021]. The IMO Guidelines aim to assist relevant authorities and stakeholders in ensuring that the trials of MASS-related systems and infrastructure are conducted safely, securely, and with due regard for the protection of the environment. As with the EC guidelines, the IMO guidelines are only interim and will be reviewed and amended in light of the experience gained from their application, and when circumstances so warrant. The results of the regulatory Scoping Exercise have highlighted the high-priority issues and potential gaps that need addressing at the regulatory level.

### 7.8.3 Attack scenarios/simulation - security hardening

During the last decades, considerable work has been carried out aiming to represent attack scenarios via various types of graph. Threat scenario and exploitation/attack/vulnerability graphs, utilizing a set of mathematical models and algorithms, are able to construct possible attack patterns. This way hardening methods can be applied to vulnerable components. Some suggestions that might assess the challenges posed in the previous subsection are the following:

- New methods that combine active approaches, which are used to detect and analyse anomaly activities and attacks in real-time, with reactive approaches, which deal with the analysis of the

underlying infrastructure to assess an incident in order to provide a more holistic and integrated approach to incident handling.

- Use of big data, machine learning and artificial intelligence techniques and technologies for the extraction of patterns in data and the identification of abnormal behaviours.
- Novel techniques for ensuring the secure distribution and storage of all incident-related artefacts, in order to protect them from unauthorized deletion, tampering, and revision.
- Integration of state-of-the-art elements for risk prediction related to the occurrence of threats, sensor/platform allocation, and communications
- User-behaviour analytics. The technology uses big data analytics to identify anomalous behaviour by a user.
- Data loss prevention. A key to data loss prevention is technologies such as encryption and tokenization.
- Security hardening for critical maritime systems.

Attack scenarios and simulation can assist in properly modifying security hardening methodologies (e.g. [PCvdV 2017] [vdVGC+ 2016] [Clang10]) for critical maritime infrastructures, as described in the relevant challenge (see Section 7.6.11).

#### 7.8.4 Secure Maritime Communications

As argued in association with research goal 4 within Challenge 4: Maritime system communication security, ensuring the confidentiality and the integrity of the information sent to and received from maritime IT assets is essential. To this end, the design and implementation of proper encryption methods is needed. In particular, the following complementing sub-goals characterize the means and measures necessary in order to facilitate this goal:

- Better encryption in order to ensure safeguarding of data.
- Better protection measures or protocols for hardware of unmanned ships and submarines.
- Physical protection measures where unmanned equipment is in use.
- Satellite connectivity for data management.

Specifically, a methodology including support for these four sub-goals will be demonstrated in the form of a PKI service, which is being developed within WP5. We envision that this service may later be applied to autonomous ships.

#### 7.8.5 Resilience

Enforcing resilience in both the cyber and physical systems of maritime transport involves various processes, methodologies and tools, such as:

- Deployment methodologies for the critical maritime systems that follow the “resilience-by-design principle”, to inherently design systems that may resist and quickly recover from unwanted events.
- Understand the continuously evolving threat landscape of the maritime sector (and transport sector in general)
- Understand the cyber and physical dependencies with other systems or sectors and the relevant security risks.
- Deploy distributed and resilient trust management systems/platforms to support secure communications.

Resilience is therefore highly related with threat modelling, risk assessment, system hardening and trust management.

Table 6: Challenges identified in the Maritime Transport Vertical and Tools needed to address them

Challenge	Tools required for	Tools contemplated for Maritime Transport	Tools/Methods that need to be addressed
Challenge 1	Early identification and assessment of risks, threats and attack paths for critical maritime systems	Collaborative Risk Management methodologies and risk assessment tools, such as MITIGATE (D3.1, Section 5.4), CORAS (D3.1, Section 5.2) and BowTie Plus (D3.1, Section 5.2)	<p>Utilisation of effective, collaborative, standards-based, risk management methodologies and model-driven approaches to address sector-specific security requirements (Capturing risks and threats arising from the global maritime supply chain, including those associated with the port's CII interdependencies and those related to cascading effects).</p> <p>Development of stable data sets for the maritime environment.</p> <p>Adaptation of efficient cyber-attack path discovery algorithms using predictive analytics and simulation techniques to capture the interdependencies among maritime interconnected systems and support the generation of alternative attack paths, as well as their assessment in terms of risk.</p>
Challenge 2	Security hardening of maritime infrastructures, including cyber and physical systems	TypeArmor (D5.2, Section 6.2) and VTPin (D5.2, Section 6.2)	<p>Software analysis and identification of unsafe components. Provide security controls at the compiler level, and runtime security mitigations.</p> <p>Utilize binary-level analysis techniques and methodologies for program hardening with no recompilation.</p> <p>In addition, entirely program-agnostic techniques that are will be explored, such as pre-loading the binary with secure memory.</p>

Challenge 3	Resilience of critical maritime systems	MITIGATE (D3.1, Section 5.4), CORAS (D3.1, Section 5.2), BowTie Plus (D3.1, Section 5.2), PKI service (CySiMS) (D3.1, Section 7) and Secure AIS ASM endpoint (D3.1, Section 7)	Develop and implement monitoring techniques that will analyse the data, and vulnerability databases providing efficient indexing. Explore, map and address risks related to unwanted maritime security events through the generation of bow-tie diagrams.
Challenge 4	Maritime system communication security	PKI service (CySiMS) (D3.1, Section 7), Secure AIS ASM endpoint (D3.1, Section 7) and BowTie Plus (D3.1, Section 5.2)	Development of a targeted trust infrastructure. A PKI service provision to support encryption requirements to safeguard data AIS and VDES communication.
Challenge 5	Securing autonomous ships	PKI service (CySiMS) (D3.1, Section 7), MITIGATE (D3.1, Section 5.4) and BowTie Plus (D3.1, Section 5.2)	Model threats against securing maritime autonomous surface ships (MASS). Develop risk models capable of addressing heterogeneous part of autonomous ships.

## 7.9 Roadmap

### 7.9.1 Short-term plan

Based on the goals set out in the previous version of the roadmap, various research efforts have been achieved to some extent, while others are expected to be delivered by the end of the project. In particular:

Concerning the research challenge described in section 7.6.11 (Challenge 1: Early identification and assessment of risks, threats and attack paths for critical maritime systems):

- We enriched cyber-attack path discovery algorithms with machine learning techniques in order to capture more accurately the dependencies and interactions of maritime systems and to analyse more accurately the mapping of attack paths against threat agents. The preliminary results of this extension have been presented recently in [GBS+2021]. Further work is in progress to extend attack

path discovery and analysis in a situational-aware manner, in order to support adaptive risk assessment.

Concerning the research challenge described in section 7.6.12 (Challenge 2: Security hardening of maritime infrastructures, including cyber and physical systems):

- The security controls related with software hardening have been integrated into the MITIGATE platform. Relevant tools and solutions have been set up and we expect to examine new controllers to improve its capacity and eliminate possible bugs or malfunctions by the end of the project.

Concerning the research challenge described in section 7.6.14 (Challenge 4: System communication security):

A demonstrator of a maritime trust infrastructure that takes into consideration the environmental limitations of the maritime transport sector, such as network availability and communication costs, has been set up and validated. Since stability of communication is an issue, it is crucial to facilitate the availability and stability of communication solutions. As such, the solutions need to be scalable and redundant. Within this context, a challenge to be met by the end of the project is to design solutions that will be VDES-ready and will support both satellite and radio communication means. Given the need for stability and redundancy, such a design will partially address the need for achieving network availability in ship communications.

## **7.9.2 Beyond the end of the project plan**

### **7.9.2.1 Security 2025**

Concerning the research challenge described in section 7.6.13 (Challenge 3: Resilience of Critical Maritime Systems):

- Ensuring the robustness of maritime ICT infrastructures and quickly identifying and adapting to security threats are long-term research goals. They entail the development and implementation of monitoring techniques supported by AI algorithms that will analyse the data, and vulnerability databases that will ensure its better indexing. Part of this challenge is addressed by the tools to be developed for the risk assessment challenge. Such solutions are expected to be available by 2025.

Concerning the research challenge described in Section 7.6.14 (Challenge 4: System communication security):

Integration of the VDES-ready secure communications application with actual VDES devices is expected to be available in the next few years, once the VDES standard has been finalized and the hardware becomes more available for use.

### **7.9.2.2 Security 2030**

Other long-term research goals are expected to be solved, fully or partially, in a longer time period.

- Efforts to achieve unified security and safety risk management of heterogeneous components in autonomous ships are expected to benefit from the development of stable data sets for the maritime environment, such as the targeted threat models. However, unified security and safety risk management frameworks should not be expected to be available for actual use before 2030.

- Similarly, security in 5G and satellite integration for ship connectivity in autonomous ships is a longer-term challenge, as the underlying technologies (i.e. 5G-enabled, dual satellite and radio communication systems) are still expected to have a longer maturity period.
- The same holds for the goal of a comprehensive communication architecture for autonomous ships, as well as the goal for GNSS security, which are expected to benefit, over a longer term, from the development of a targeted trust infrastructure.

### 7.9.3 Milestones

By the end of the project, the vertical is expected to reach the following milestones:

- Prototype of the maritime transport security demonstrator

## 7.10 Summary

This section focuses on security for the EU maritime transport. Maritime transport or else “Blue economy” is a powerful means for the EU, which is directly linked with a number of industries and which is considered as one of the cornerstones of the EU economy and growth. As modern maritime transport infrastructures are getting increasingly digital, they generate cyber-dependencies among them and they facilitate the communication between dispersed nodes. In this vein, such infrastructure dependencies attract the attention of sophisticated adversaries and give them the opportunity to conduct multi-vector attacks to compromise cyber-physical maritime transport systems that can possibly cause a tremendous impact in the maritime transport ecosystem, e.g. economic loss, environmental impact, such as the shipping and logistics giant’s Maersk NotPetya attack in 2017 disrupting critical systems and causing financial loss of \$200-300 million (see sections 7.4 and 7.5 for major maritime transport incidents and the threat agents’ profile of the current vertical).

A bird’s eye view on the state of the art (section 7.6.1) of the maritime transport security ends up with open issues regarding the need to invest more on maritime transport cybersecurity research, in terms of:

- further investigating maritime cybersecurity legal aspects, developing solutions and conducting trainings (i.e. cyber ranges) that raise the security awareness of the maritime transport stakeholders;
- thoroughly examining the diverse set of communication interactions in the shipping Industry;
- focusing on balancing infrastructure resilience and cost optimization; and
- creating a risk management culture according to the specific security requirements of the EU maritime transport environments.

Within this framework, the final goal is to set policies and strategies that ensure the security enablers, including, confidentiality, integrity, availability, authenticity, accountability, non-repudiation, and finally reliability of the maritime transport systems, while at the same time increasing the sector’s situational awareness to maintain security in the overall EU maritime transport ecosystem (section 7.6.2). In this light, maritime transport key players could increase their agility and preparedness against unwanted threat events

and this could pave the way to establish a resilient maritime transport industry, which could strengthen the EU economy and reinforce the EU digital sovereignty (section 7.6.3).

To provide a more clear view on the current maritime transport security status in the EU, a SWOT analysis has been conducted and has shown that as maritime transport is a critical sector for the European economy, EU gradually increases investment on maritime transport cybersecurity research as a stepping stone to advance its growth and promote digital sovereignty to build sustainable maritime transport environments against the emerging threat landscape. In addition, EU has been focused on setting recovery plans and respective security actions on the maritime transport to address the COVID-19 pandemic crisis that has threatened the global welfare and promote the public health (section 7.6.4) and to respond to the Green Deal environmental requirements (section 0) and climate change variables (section 7.6.6) that have led to new technology trends as a means to reshape the global economy. Furthermore, the pandemic disease (i) has significantly reduced the maritime transport cargo and passengers' movement across and beyond the borders of Europe and (ii) has raised the trend of teleworking (section 7.6.4). Thus, reinforcing security in the e-maritime environment could help to amplify the Europe's strategic autonomy (section 7.6.3).

Criminality has plagued the maritime transport sector over the years, as that sector is a major means of transport that could support malicious activities, such as the illegal transfer of goods and people (e.g. smuggling, human trafficking), diffuse carriage of chemicals, the release of dangerous substances to cause environmental degradation, etc. The trend towards digitalisation in maritime transport within the past decades has attracted the attention of adversaries, who may wish to exploit the vulnerabilities of ICT and OT systems and take advantage of the monitoring of such systems in order to promote the kind of malicious activity mentioned above, or even develop new crimes (e.g. hacking and manipulating autonomous vessels could lead to their collision). Hence, cyberattacks on maritime transport CIs can enable criminals to disturb global trade, food security and tourism (freedom of movement), as well as threatening human life, which can reduce human rights, limit other types of benefits and thus degrade democracy (section 7.6.7).

The new EU Cybersecurity Strategy, published in December 2020, sets out how the EU will shield its people, businesses and entities from the emerging cyber threat landscape, and promotes global collaboration and security for a global and open Internet. Within this framework, in the current vertical it has been investigated whether and how the maintenance of maritime transport cybersecurity can contribute to the EU CyberSecurity Strategy for the Digital Decade, with regard to the specific topics (section 7.6.8) presented below:

- Resilient infrastructure and critical services
- Building a European Cyber Shield
- An ultra-secure communication infrastructure
- Securing the next generation of broadband mobile networks
- An Internet of Secure Things
- Greater global Internet security
- A reinforced presence in the technology supply chain
- A cyber-skilled EU workforce
- EU leadership on standards, norms and frameworks in cyberspace
- Cooperation with partners and the multi-stakeholder community
- Strengthening global capacities to increase global resilience

Considering all these different cybersecurity aspects that have been analysed for the Maritime Transport sector, it has been concluded that Maritime Transport is a critical Industry sector in the EU and the maintenance or either the accidental or deliberate compromisation of its cybersecurity can have a direct impact to the EU economy and to the safety of the environment, public health and human life outside and within the EU. Therefore, it is a top priority to invest in the protection of EU maritime critical infrastructures aiming to maintain their security and increase the sectorial preparedness over security incidents. As a consequence, that could implement the big picture; the provision of a resilient EU maritime ecosystem (section 7.1).

The current research roadmap aimed at identifying the most important research security challenges that have to be deeply investigated and addressed in order to create a pathway to the previous described vision (section 7.1). The roadmap (section 7.9) has been identified in short-term plan (by the end of the project, cf. section 7.9.1) and long-term plan (beyond the end of the project, cf. section 7.9.2) mapping the addressed research priorities to the future (security 2020 and security 2030 cf. section 7.9.2) The most prominent challenges in the maritime transport security are considered (section 7.6):

- Challenge 1: Early identification and assessment of risks, threats and attack paths for critical maritime systems
- Challenge 2: Security hardening of maritime infrastructures, including cyber and physical systems
- Challenge 3: Resilience of critical maritime systems
- Challenge 4: Maritime system communication security
- Challenge 5: Securing autonomous ships

The identified challenges have been mapped on to the big picture, and methods, mechanisms and tools have been proposed to address them (section 7.8). Moreover, promising risk management and threat modelling methodologies for maritime transport should be able to explore the sector-specific security requirements and the cascading effects involved in risk implementation, in order to provide stable data sets for the maritime environment (Challenge 1). In addition, a software analysis to identify possible unsafe components, the implementation of security controls at the compiler level and runtime security mitigations could provide accurate results useful for hardening maritime infrastructure systems (Challenge 2). The development of a targeted trust infrastructure providing a PKI service to cover encryption requirements (which improves physical and cyber protection measures and provides secure satellite connectivity) could ensure the digital data protection of maritime communications (i.e. AIS and VDES) (Challenge 4). The provision of security among autonomous ships could be addressed with the adoption of optimal risk models that capture the threat landscape of unmanned vessels holistically (Challenge 5). The accomplishment of all the previous proposals could create a resilient maritime transport environment. Such an environment should incorporate a “resilience-by-design” agile system that responds quickly to security incidents, is aware of the evolving sectorial security threat surface, considers interdependencies among infrastructures and the consequences for risk propagation, and deploys trust management systems to secure maritime communications (Challenge 3).

## 8 Medical Data Exchange

### 8.1 The Big Picture

When citizens browse on the Internet, use connected devices and wearables, and do online business, they generate an enormous amount of data. On the other hand, when companies and public organizations (health, education, legal, etc.) provide online services, they also require and generate a massive quantity of data. In both cases the trend is to grow more. In the case of the health domain, a huge amount of data is generated year by year, reaching around 10 petabytes (PB) per year<sup>343</sup>. This enormous amount of stored data can be used by their producers (individual citizens, wearable companies, hospitals, health organizations, pharma laboratories) improving citizens' health. The value of this information increases when is shared with others. A medical data exchange platform can sharply increase the value of these data, gathering data providers and data consumers in a single place. Additionally, the possibility of cross-border exchange of data, due to the increase of cross-border businesses gives an added value to these data.

Different kind of data (financial, statistic, scientific, education, personal or health data) can be stored and shared between parties. Health data is a kind of sensitive data that must be managed with special care. The management and access to these sensitive data on the data exchange platforms need to be appropriate in terms of quality, security and privacy. The medical data exchange platform must assure the integrity and reliability of the data. Additionally, only allowed users will get access to the platform where the data or metadata are stored. Also, the data must be protected at any moment when transiting between parties. Moreover, during the sharing process the user data privacy must be preserved at any moment. Furthermore, in order to engage new users to the platform willing to share and consume data, both the data consumers and data providers must interact with the exchange platform in a friendly way. Finally, the platform must fulfil with the current legislation assuring the user rights and the data protection accomplish. These measures will prevent a third party to learn from user data, providing a secure and smooth use of the medical data exchange platform. In the context of Medical data exchange demonstrator these aspects will be addressed.

### 8.2 Overview

According to Forbes<sup>344</sup> more than 2.5 quintillion bytes of data were created each day during 2018; 463 exabytes of data per day are expected in 2025<sup>345</sup>. Data assets in healthcare domain are growing fast than in other sectors<sup>346</sup>. Tons of health data and medical records are produced every day. Wearables generate massive amounts of data each second, while hospitals and primary healthcare centres collect huge amount of records every day. Additionally, the number of medical imaging tests, blood and genetic tests, increases constantly. Overall, the big data health market will achieve a very important volume as healthcare data are expected to have a compound annual growth rate (CAGR) of 36%<sup>347</sup>.

---

<sup>343</sup> [https://www.dellemc.com/en-tz/collaterals/unauth/briefs-handouts/solutions/h17823\\_solution\\_brief\\_driving\\_real\\_clinical\\_business\\_outcomes\\_with\\_a\\_modern\\_it.pdf](https://www.dellemc.com/en-tz/collaterals/unauth/briefs-handouts/solutions/h17823_solution_brief_driving_real_clinical_business_outcomes_with_a_modern_it.pdf)

<sup>344</sup> <https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/>

<sup>345</sup> <https://www.raconteur.net/infographics/a-day-in-data>

<sup>346</sup> <https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf>

<sup>347</sup> <https://healthitanalytics.com/news/big-data-to-see-explosive-growth-challenging-healthcare-organizations>

The health system overall can be significantly improved when these medical data are shared among health stakeholders, data producers (e.g. hospitals, primary healthcare centres, health clinics, clinical analysis laboratories), citizens (as health data providers), and data consumers (e.g. research institutions, health authorities, pharmaceutical industry, drug agencies, insurance companies). Such sharing is possible through a data exchange market platform that shares data between different stakeholders. The data exchange platform provides data consumers access to data shared by the data providers.

Conversely, a lack of data sharing has a negative impact on the development of computer-based solutions. This negative impact affects areas such as imaging-based machine learning technologies which (i) are able to simulate surgical treatments or device implants, (ii) are able to automatically detect pathological lesions and (iii) are able to cross-reference imaging findings with other patient data for highly personalized clinical predictions. The data required for developing and testing these systems exists today in large quantities inside hospital firewalls<sup>348</sup> [RCT+ 2018] [YWC 2018], but it cannot be accessed without jeopardizing patient privacy and exposing institutions to severe legal implications.

The GDPR has established a much-needed legal framework that sets clear boundaries for compliant data exchanges and provides clear guidance to economic players, finally framing biomedical data sharing within legal boundaries and opening the possibility for trading such data under different classifications and corresponding legal agreements. The issue still to be solved is the need for a robust and scalable solution to enforce privacy and security requirements in a way that efficiently meets the strong demand for health data.

The medical data exchange demonstrator, leveraging an existing data exchange marketplace (Dawex<sup>349</sup>), will tackle these challenges and contribute to the setting up of a trusted and secured data exchange platform in Europe for medical data.

## 8.3 What is at stake?

Medical data sharing platforms manage personal and sensitive data that must be protected and whose privacy must be preserved. An overview of what needs to be protected and which are the main risks and scenarios when this data is compromised is provided in the next sections.

### 8.3.1 What needs to be protected?

The main asset to protect is the **health data** generated by several providers, such as citizens, patients, doctors, hospitals, governmental and pharmaceutical organizations, research institutions and private health institutions. The health data collected is generated by wearable health devices that collect a user's personal health and exercise data, patients' devices that collect medical data, diagnostic image devices, online diagnostic tools, medical research, clinical trials, pharmaceutical research, etc.

---

<sup>348</sup> <http://www.appliedclinicaltrials.com/how-ehrs-facilitate-clinical-research>

<sup>349</sup> <https://www.dawex.com/es/>

As the health data generated is of a personal nature, it is protected and is not provided to data consumers. Only the associated **metadata** that is closely related with health data is displayed on the data exchange marketplace to be browsed.

It is not only health data that needs protection: apart from sensitive medical data, the **personal data** that could be associated with this data and the personal data from the different data exchange stakeholders (data providers and data consumers) must also be protected.

Moreover, a suitable technology and infrastructure are also essential requirements for developing the data sharing process in a secure way. Hence, the security and privacy of health information must be assured, not only during data **storage**, but also during the **exchange** and/or **sharing processes**<sup>350</sup>.

### 8.3.2 What is expected to go wrong?

In a sector such as health data exchange, where sensitive data is managed, all the players/stakeholders involved must be aware of the risks when managing this kind of data. For this reason, the use and development of security and privacy tools, compliance with regulations and observance of standardized procedures are essential for preventing things from going wrong. Because of the significance of this kind of data, the health care sector in general has become a clear target for cybersecurity attacks.

Healthcare data breaches reported in the USA have increased sharply in recent years (2009-2018), from 18 cases during 2009 to one case per day during 2018<sup>351</sup>. According to the 2019 Data Breach Investigations Report performed by Verizon<sup>352</sup>, which included data from 86 countries around the world, 466 incidents were reported, of which 304 declared data disclosure.

Intentional hacking, IT incidents, unauthorized data access/disclosure, theft, loss and even inadequate disposal are the main threats. Additionally, ECSO in the Healthcare Sector Report points out that the “use of cloud services, unsecure networks, employee negligence, bring your own device (BYOD) policies, lack of internal identification and security systems, stolen devices with un-encrypted files and others<sup>353</sup>”, are potential causes of data breaches. Unfortunately, the leading causes of breaches that occurred this year in the UK were related to human error (incorrect disclosure to wrong recipient or replying to a phishing attack), followed by wrong data shown, loss, theft or even direct communication of personal data<sup>354</sup>. Attacks on personal devices (wearables, medical devices), when updated on unsecure or compromised networks, are also worth mentioning.

Although addressing all of these data breaches is challenging, a continuous evaluation of the services, tools, standards and procedures developed for the data sharing process while managing the medical data exchange platform will help to avoid or minimize these attacks, while improving the confidence and trust in these solutions for citizens and patients sharing the data.

---

<sup>350</sup> [https://www.researchgate.net/publication/234034137\\_Protecting\\_Patient\\_Privacy\\_when\\_Sharing\\_Medical\\_Data](https://www.researchgate.net/publication/234034137_Protecting_Patient_Privacy_when_Sharing_Medical_Data)

<sup>351</sup> <https://www.hipaajournal.com/healthcare-data-breach-statistics/>

<sup>352</sup> <https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief-emea.pdf>

<sup>353</sup> <https://www.ecs-org.eu/documents/publications/5ad7266dc1c8a.pdf>

<sup>354</sup> <https://www.healthcareitnews.com/news/europe/statistics-reveal-healthcare-sector-most-affected-personal-data-breaches>

### 8.3.3 What is the worst thing that can happen?

In the medical data exchange scenario, the main kind of impacts are related to the following aspects:

- User privacy;
- Integrity of the data;
- Data breach;
- GDPR compliance.

Considering these aspects, the worst-case scenarios are as follows:

- Sensitive data and health records can be stolen by intruders if the security mechanisms fail.
- Recurrent data breaches will occur if the system is not secure enough or the control and tracking of activities on the platform are not well monitored and checked appropriately.
- Users' private data may be lost if data is exposed to the public. The loss of sensitive data belonging to citizens and patients will mainly cause privacy issues. Depending on the final recipient of this data, the user's normal life can be affected in different ways. If these sensitive records (health records, genetic information) reach insurance companies, they could leverage this information to justify increasing premiums, charging extra payments or even rejecting users who have health problems.
- Public health IT infrastructure may suffer crashes if software or hardware vulnerabilities are exploited by malicious third parties.
- Loss of life may occur when IT health infrastructures are endangered and the integrity of the data is compromised, if data is lost or not available to health personnel (doctors, nurses, care assistants, etc.) on emergency cases.
- Trust and confidence from users, data providers and data consumers may be compromised if data sharing platforms manage the stored data in an inappropriate manner.
- Considerable fines may be imposed if a data sharing platform fails to comply with the applicable regulations, such as GDPR.
- Financial losses may be caused by one of more of the above scenarios. According to the GDPR regulations, data breaches are penalized by EU Member State authorities<sup>355</sup>, as personal or sensitive data are made public.

## 8.4 Who are the attackers?

As confidential and sensitive information is managed and stored by data sharing platforms, cyber-attacks against these platforms have been steadily increasing in number during recent years. Techniques such as SQL injection, zero-day attacks, malware, ransomware and advanced persistent threats (APT) are being used. The most common attackers who are using these technologies are the following:

---

<sup>355</sup> <https://gdpr.eu/fines/>

- **Hackers**, as cyber criminals holding a company or hospital’s data hostage while money is not paid, using ransomware, or the use of APT for obtaining personal health data to sell on the black market/dark web;
- **Hactivists**, acting for political reasons or against the practices of some pharmaceutical companies;
- **Economic adversaries** (foreign companies, states) willing to undermine their competitors by exposing their vulnerabilities;
- **White hat**, willing to help companies and organizations identify and fix their security flaws;
- **Cyber-terrorists** from foreign states, willing to destabilize the public health infrastructure of the countries they target;
- **Insiders**, unauthorized employees accessing the system, network or databases, aiming to make fraudulent use of data. Contractors and even users could be placed in this group. The access could be accidental when the employee is a victim of phishing, but it can cause a serious data breach. Negligence, operational errors or mistakes performed by employees can also cause unintentional data loss.

Special care needs to be paid when the health data is managed by private companies. Recently, Project Nightingale<sup>356</sup> has been involved in a “secret transfer of medical history data, which can be accessed by Google staff”<sup>357</sup>. Apparently, health data has been delivered, including personal data. Therefore, not only security measures must be put in place to prevent attacks from external attackers, but measures must also be taken to avoid personal and sensitive data being made public by internal staff.

As indicated before cybersecurity practices must be followed to manage threats and preserve personal and sensitive data<sup>358</sup>.

## 8.5 Major incidents in this vertical

The increased number of digital healthcare services (medical devices, medical data stored by hospitals and cloud services) has made medical treatments faster and more precise. This digital transformation of the health domain, which manages sensitive data, has turned the health industry into a target for malicious attacks, both internal and external. Data breaches affect citizens, public and private health organizations, and health businesses [SZA+ 2020].

In recent years, the healthcare domain has become the most attractive target for cybersecurity attacks. Ransomware and phishing are the most common techniques used. The cost for containing and recovering from these attacks can reach millions of euros. Indicatively, 400 healthcare companies reported a data breach in 2019— a record for healthcare organizations.<sup>359</sup> An increase of 10 to 15% is expected in the near future [FHS 2020].

Some of the major healthcare data breaches have been:

---

<sup>356</sup> <https://www.theatlantic.com/technology/archive/2019/11/google-project-nightingale-all-your-health-data/601999/>

<sup>357</sup> <https://www.theguardian.com/technology/2019/nov/12/google-medical-data-project-nightingale-secret-transfer-us-health-information>

<sup>358</sup> <https://tinyurl.com/r37vb7o>

<sup>359</sup> <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-data-breach>

- **Anthem Health Insurance 2015.** Personal data records (name, birth date, medical ID/Social Security number) were stolen from 78.8 million users.<sup>360</sup>
- **Premera Health Insurance 2015.** Medical information from 11 million users was exposed.<sup>361</sup>
- **Excellus Health Insurance 2015.** Medical data, Social Security numbers and financial information of more than 10 million user was compromised.<sup>362</sup>
- **NHS 2018.** The National Health Service in the UK suffered a WannaCry ransomware attack in May 2018. In a single week, 19,000 appointments were cancelled, and restoration of data and systems cost more than £90 million.<sup>363</sup>
- **HSE 2021.** The Irish Health Service Executive network suffered a Conti ransomware attack, shutting down the IT systems of hospitals, clinics and health providers and affecting about 5 million people.<sup>364</sup>
- **Italian COVID-19 vaccination booking system 2021.** An Italian health portal used to schedule COVID-19 vaccination appointments was breached and encrypted using ransomware. Reportedly, no data were retrieved, and vaccinations could continue for those who already booked an appointment, but new appointments were not possible until the system was restored.<sup>365</sup>

These examples of cybersecurity issues affecting the healthcare domain impact on the integrity of the IT health systems and the patients' privacy. This implies not only monetary losses and data breaches but also a risk to patient's lives.<sup>366</sup>

## 8.6 Research Challenges

Research on different aspects and technologies, such as privacy, security, access control, trust and crypto technologies, are needed in order to avoid the previously described scenarios. Since the GDPR regulation<sup>367</sup> came into force in 2016 and was applied on 25<sup>th</sup> May 2018, additional research must be developed in the data sharing domain, including tools and actions that guarantee users can exercise their rights when personal and sensitive data are processed.

### 8.6.1 State of the Art

The previous version of this document [Markatos 2020] specified the resources that have to be protected in the field of medical data exchange, the vulnerabilities and threats that exist, and the potential attackers. Based on these, the main challenges were defined (sections 8.8.1 – 8.6.14), focusing on the security of medical data, the preservation of the privacy of data when it is shared, the trustworthiness of the entire process of exchanging medical data, regulatory considerations, and, finally, the challenge of visually

<sup>360</sup> <https://www.insurance.ca.gov/0400-news/0100-press-releases/anthemcyberattack.cfm>

<sup>361</sup> <https://www.trendmicro.com/vinfo/fr/security/news/cyber-attacks/premera-blue-cross-data-breach-exposes-11m-patient-records>

<sup>362</sup> <https://eu.usatoday.com/story/tech/2015/09/10/cyber-breach-hackers-excellus-blue-cross-blue-shield/72018150/>

<sup>363</sup> <https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf>

<sup>364</sup> [https://cyberlaw.ccdcoe.org/wiki/Ireland%E2%80%99s\\_Health\\_Service\\_Executive\\_ransomware\\_attack\\_\(2021\)](https://cyberlaw.ccdcoe.org/wiki/Ireland%E2%80%99s_Health_Service_Executive_ransomware_attack_(2021))

<sup>365</sup> <https://www.bleepingcomputer.com/news/security/ransomware-attack-hits-italys-lazio-region-affects-covid-19-site/>

<sup>366</sup> <https://www.cisecurity.org/blog/cyber-attacks-in-the-healthcare-sector/>

<sup>367</sup> [https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en)

representing large quantities of medical data. To address and/or further the research into solving these challenges, methods, mechanisms and tools (sections 8.7.1 – 8.7.5) produced or used as part of CyberSecurity4Europe project have been identified.

This section discusses the state of the art of the technologies, methods, mechanisms and tools developed and/or used in this project to advance the topics related to medical data exchange. As mentioned before, a considerable part of this research is performed by this project, and consequently, some of the state of the art might have already been discussed in other deliverables [Skarmeta 2019]. For this reason, a shorter description is given, together with a note as to where the full state of the art can be found (as well as more information on the developed solution).

### 8.6.1.1 Identity management and eIDs

Identity management and electronic IDs are important for medical data exchange from the perspective of efficiently tracking the same patient's data across different systems, while ensuring the protection of patients' privacy and security as well as the integrity of their data (see challenge 1 and partially challenge 3).

Traditional identity management is based around trusted central authorities, which hold user identities for a given domain. As a result, the users cannot sign on across different domains using the same credentials, while the systems become vulnerable to threats such as data breaches, identity theft and other privacy concerns. The evolution of this type of system was the federated models that enabled Single Sign-on. These newer systems allow users to use the same identity across multiple domains and mitigate some of the previous vulnerabilities. Several solutions, such as OpenId<sup>368</sup>, SAML<sup>369</sup> and FIDO<sup>370</sup>, have been developed to be used as a baseline for such systems.

A modern approach based on self-sovereign identities<sup>371</sup> focuses on providing a privacy-respectful solution, enabling users to have full control and management of their identity data without needing a third-party centralized authority to manage their identity. Thus, the users become data controllers of their own identities and can directly manage their personal data during online transactions. Furthermore, identity management with self-sovereign identities has been combined with blockchain technologies to provide governance of the system, improving the performance to be usable on a large scale and enabling access to identities for everyone.

Blockchain enables sovereignty, as users can be endowed with means to transfer digital assets, including user-decentralized identifiers [RMD+ 2020], documents related to decentralized identifiers, identity attributes, verifiable claims and proofs of identity [SD 2017], to anyone privately. The latest blockchain solutions [TD 2016] [BNM+ 2014] make use of distributed ledger technologies, along with user-centric and

---

<sup>368</sup> <https://openid.net/>

<sup>369</sup> J. Hughes and E. Maler, Security assertion markup language (saml) v2.0 technical overview, OASIS SSTC Working Draft sstc-saml-techoverview-2.0-draft-08, pp. 29-38, 2005

<sup>370</sup> <https://fidoalliance.org/fido2/>

<sup>371</sup> A. Tobin and D. Reed, "The inevitable rise of self-sovereign identity," tech. rep., The Sovrin Foundation, 2016. <https://sovrin.org/wpcontent/uploads/2017/06/The-Inevitable-Rise-of-Self-SovereignIdentity.pdf>

mobile-centric approaches. The main self-sovereign identity concepts on blockchain and their future were described by K. Wagner et al. [WNR+ 2018].

A more detailed overview of the state of the art in the field of identity management, is presented in D3.11 *Definition of Privacy by Design and Privacy Preserving Enablers*, section 3.2.2 *Identity Management* [Sforzin 2020].

When dealing with medical data, challenging issues are also posed by EU citizens moving across national borders but still requiring healthcare services. In this project, we primarily focus on the problem of the employment of eIDs and their interoperability (as regulated by eIDAS). Currently, the use of national eID schemas for authentication purposes against public online services is mandatory<sup>372</sup> and is widespread in each country<sup>373</sup>. But despite several projects having been launched by EC (e.g. LEPS, eIDAS2Business), the use of eID in the private sector is still very low.

The EC has been focusing on boosting the use of eID among SMEs during the last few years<sup>374</sup>. Initiatives such as go.eIDAS<sup>375</sup> are addressing the use of eID with trust services (signing, timestamp, etc.). Examples such as the CEF<sup>376</sup> LEPS<sup>377</sup> EU project show how postal services from Spain and Greece, and the Hellenic Exchanges-Athens Stock Exchange (Athex) company from Greece leverage the eIDAS network by using the eIDs issued by the EU Member States in their registration process. A recent initiative [BLC 2020], which provides login and Wi-Fi access services by using the eIDAS network, has shown benefits for users and service providers.

Currently, the EC is trying to integrate new building blocks (e.g. blockchain), with eIDAS. The project European Self Sovereign Identity Framework (eSSIF)<sup>378</sup> is part of the EC supported European blockchain service infrastructure (EBSI), for using blockchain technologies within online public services. Several other projects, such as the eSSIF-Lab for increasing the uptake of the Self-Sovereign Identities (SSI) on cross-border online transactions<sup>379</sup>, are also funded by the European Union. The goal in this project is to ease the use of the eIDs enabling cross-border authentication to medical services.

A more detailed overview of the authentication efforts related to eIDAS within the EU, is delineated in D3.11, section 3.2.5 *Authentication* [Sforzin 2020].

In June 2021 the European Commission proposed to set up a new trusted and secure Digital Identity framework<sup>380</sup> based on trust, security and interoperability principles. This proposal implies that EU citizens and residents can identify themselves and share electronic documents, such as a driving license, by using

---

<sup>372</sup> <https://ec.europa.eu/digital-single-market/en/e-identification>

<sup>373</sup> <https://ec.europa.eu/digital-single-market/en/eu-trusted-lists>

<sup>374</sup> <https://ec.europa.eu/digital-single-market/en/eidas-smes>

<sup>375</sup> J. Schwenk, <https://blog.eid.as/welcome-to-the-future-of-trust/> 2019.

<sup>376</sup> <https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/2016-eu-ia-0059>

<sup>377</sup> <http://www.leps-project.eu/>

<sup>378</sup> [https://www.youtube.com/watch?v=P5xjnWL3Pg0&ab\\_channel=SSIMeetup](https://www.youtube.com/watch?v=P5xjnWL3Pg0&ab_channel=SSIMeetup)

<sup>379</sup> eSSIF-Lab, Working for development, integration and adoption of Self-Sovereign Identities (SSI) technologies.

<https://essif-lab.eu/>

<sup>380</sup> [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_21\\_2663](https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2663)

their European Digital Identity wallet. In this way a citizen can easily access those private or public EU online services that require a strong authentication, using their smart phone. This initiative increases user privacy, as the user has control of the information shared or delivered to third parties. In this context Estonia is in the lead of the European digitalisation process.<sup>381</sup>

### 8.6.1.2 Medical data privacy

One of the main issues when personal and sensitive data, such as health data, are shared is that of privacy. Privacy-preserving techniques have been developed in this project to maintain user data (challenge 2), as well as building on the trustworthiness of the entire system (challenge 3), which is especially the case for techniques of anonymization. Anonymization or de-identification is a vital part of managing medical data, because it enables the sharing of data for secondary purposes. Secondary purposes are primary purposes that are not related to providing patient care, such as research, teaching, public health and marketing.

Anonymization can be performed using various algorithms, as well as a wide variety of privacy models<sup>382</sup>. For example, k-Anonymity, k-Map,  $\delta$ -presence, risk-based privacy models, differential privacy and the game-theoretic model are privacy models commonly used for attributes that are going to be transformed. In contrast, l-diversity, t-closeness,  $\beta$ -likeness and  $\delta$ -disclosure privacy are privacy methods to be used on sensitive attributes. Some models further require particular settings (e.g. a value generalization hierarchy must be specified to be able to use t-closeness with hierarchical ground distance). Some privacy models (e.g. k-map [El Emam 2008] and  $\delta$ -presence [Ercan 2007]) require a population table.

The anonymization can be done in a static or in a dynamic way. In the more traditional, static approach, data is anonymized before it is managed. This has the advantage of being easier to implement, but also brings drawbacks primarily related to adaptivity and accuracy<sup>383</sup>. With the dynamic approach, the data anonymization is a part of the data query process. Given the spectrum of anonymization possibilities, some experts believe that the dynamic/interactive anonymization tools assure privacy at a more optimal level than static tools. Given the large parameters to be taken into account (data usability versus data protection), the probability of generating good (useful) anonymized data with static anonymization is lower.

Several anonymization tools are available on the market: e.g. Aircloak Insights, Amnesia, Anonimatron, Anon-Tool, ARX, Cornell Anonymization Toolkit (CAT), DiffprivR toolbox, FLEX, GUPT, Open Anonymizer, PINQ and wPINQ, PPS, PSI, RAPPOR, sdcMicro, SECRET, TIAMAT, UTD Anonymization Toolbox, and  $\mu$ -ARGUS.

One of the biggest advantages of data anonymization is that when the data set is properly anonymized, the data can be used freely, i.e. it can be shared or transferred without being protected by GDPR or any other regulation. However, in some cases, the anonymization is not possible. In such cases, the data must be protected in a proper way, applying a particular pseudonymization procedure, and be covered by the corresponding legislation measures. Similarly, pseudonymization is used to protect personal data, since anonymization processes are difficult. But pseudonymous data are still considered as personal data under

---

<sup>381</sup> <https://e-estonia.com/estonia-the-eid-pioneer-reacts-to-the-european-digital-wallet-plans/>

<sup>382</sup> <https://arx.deidentifier.org/overview/privacy-criteria/>

<sup>383</sup> N. Sartor. Data Anonymization Software – Differences Between Static and Interactive Anonymization, 2019.

GDPR, and the related security procedures have to be applied. Therefore, when using non-anonymized data, it is necessary to follow the appropriate data protection requirements, i.e. GDPR.

A further state-of-the-art analysis of the existing anonymization techniques and the abovementioned anonymization tools is presented in D3.11, section 3.2.5 *Anonymization* [Sforzin 2020].

Functional encryption is a generalization of public-key encryption, which allows users to delegate to third parties the computation of specific functions of the encrypted data without them learning anything else about the data by generating specific secret keys for these functions [BSW 2011]. Unlike standard encryption schemes, which work on the all-or-nothing premise, where the data is either encrypted or decrypted, functional encryption allows for fine-grained control of the decryption capabilities of third parties. This can be very useful because it allows the intentional disclosure of some information from the encrypted data to a specific key holder. For example, it could be used to get an average value of some of the encrypted values without revealing the data itself, or to reveal just a tiny and specific part of the plaintext. This could come in especially handy, since regulations like GDPR have very strong limitations on third party processing, which could be avoided if the third parties never get to process the private data itself. Functional encryption includes and unifies many other advanced encryption paradigms that used to be studied independently, such as identity-based encryption, searchable public-key encryption, hidden-vector encryption, identity-based encryption with wildcards, attribute-based encryption, and inner-product functional encryption.

Probably the most prominent type of functional encryption, and also the most relevant in Crypto-FE (section 8.7.2), is attribute-based encryption (ABE). Attribute-based encryption is further divided into the Key-Policy ABE and the Ciphertext-Policy ABE [GPS+ 2006]. In the former, the user's private key corresponds to an access policy and the ciphertext corresponds to a set of attributes. If the attributes satisfy the access policy, the user can decrypt correctly. In the latter, with Ciphertext-Policy ABE, the user's private key is generated under a set of attributes and the ciphertext is linked with an access structure. If the attributes satisfy the access structure, the user can decrypt correctly [DMK 2020].

There are several advantages of ABE<sup>384</sup>, and many are very relevant to medical data exchange. First of all, access control with cryptography (i.e. ABE) provides greater security assurance than software-based solutions and is more privacy-preserving (by default everything is encrypted – only the holders of specific attributes can gain access or read the information). This solution is also efficient in the use of space, as the same encrypted data are used by everybody, unlike typical public-key encryption, where data would have to be encrypted for each user separately. ABE is especially convenient for widely distributed data, access to which must be limited, as in the case of the Internet of Things (IoT). It also allows for the introduction of access policies after the data have already been protected, which makes it easily adjustable to any future requirement changes.

Implementations of attribute-based encryption are still fairly rare, and they are not as well established as the libraries for standard encryption schemes. There have been a fairly small number of research efforts or

---

<sup>384</sup> Sophia Antipolis. ETSI releases cryptographic standards for secure access control. 2018. <https://www.etsi.org/newsroom/press-releases/1328-2018-08-press-etsi-releases-cryptographic-standards-for-secure-access-control>

experimental implementations (for example [LOS+ 2010] [HKN+ 2015] [HKN+ 2016] [PM 2018]). Ziskau S. et al. [ZTB+ 2016] have compiled a list and an overview of existing implementations including cpabe<sup>385</sup>, libfenc<sup>386</sup>, and Charm<sup>387</sup>. Possibly the most relevant new implementation since then (excluding the results from the FENTAC project<sup>388</sup>, which include Crypto-FE<sup>389</sup>) is the OpenABE library<sup>390</sup>. A list of additional ABE implementations can be found on GitHub<sup>391</sup>.

According to a wide review of recent security and privacy studies [OSL 2021], the following trends and challenges have been identified:

- More efficient, faster and lightweight cryptosystems are needed, in view of the huge increase of e-health data produced by health services, smart healthcare devices and medical images;
- Research on re-identification when medical data are shared. In this way data anonymization techniques can be evaluated in terms of resistance to re-identification;
- Use of blockchain for securing medical data and assuring data integrity, auditability and accountability.

### 8.6.1.3 Legal and regulatory considerations

Compliance with the common European regulatory rules, especially those related with privacy when sensitive data are shared, will facilitate the cross-border data exchange of medical data (challenge 4). A specific requirement of GDPR, the production of which we wish to address in this project, is the Data Protection Impact Assessment (DPIA is significant in medical data exchange because medical data are considered a special type of personal data and assessment is therefore required (when processing non-anonymized data).

A search for GDPR guides will return many results, but the majority of them are just a synopsis of the regulation without any additional information. The most important guidelines on GDPR are the GDPR Guidelines, Recommendations, and Best Practices<sup>392</sup> from the European Data Protection Board (EDPB) and those previously made by the Article 29 Working Party (WP29), which the EDPB has since endorsed. The second important sources of guidelines are the guidelines and recommendations from national data protection agencies. These are especially useful, because they take into consideration any additional national/local legal requirement and/or recommendations. An excellent example of these are the guidelines from the United Kingdom's Information Commissioner's Office (ICO)<sup>393</sup>, which were created before they left the EU, but are still relevant. The Data Protection Commission of Ireland has issued guidelines<sup>394</sup> (they are used as an example, because they are in English and understandable to the readers of this document), as

---

<sup>385</sup> <http://acsc.cs.utexas.edu/cpabe/>

<sup>386</sup> <https://code.google.com/archive/p/libfenc/>

<sup>387</sup> <http://charm-crypto.io/>

<sup>388</sup> <https://fentec.eu/>

<sup>389</sup> <https://github.com/fentec-project/abe-wrappers>

<sup>390</sup> <https://github.com/zeutro/openabe>

<sup>391</sup> <https://github.com/topics/attribute-based-encryption>

<sup>392</sup> [https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices\\_en](https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en)

<sup>393</sup> <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>

<sup>394</sup> <https://www.dataprotection.ie/en/organisations>

have other EU countries' Data Protection Authorities<sup>395</sup>, but they are generally not as detailed as the UK's. The Guidelines produced by CyberSec4Europe will offer the most important of these recommendations in a comprehensive way and with the possibility of performing a DPIA along the way.

Likewise, there exist only a few good practices, recommendation lists, and tools to help organisations implement DPIAs. The list of available solutions designed to help perform the DPIA, discussed in the rest of this section, is limited to those freely available and excludes the commercial ones, especially as the goal is to provide a solution for smaller organisations that cannot allocate a considerable amount of resources to performing a DPIA. Existing general tools for performing a DPIA include the DPIA template<sup>396</sup> by the ICO of the United Kingdom, the tool<sup>397</sup> of the European Union Agency for Cybersecurity (ENISA), and the PIA software<sup>398</sup> provided by the French supervisory authority Commission Nationale de l'Informatique et des Libertés (CNIL). However, there are also solutions that were created for a specific use-case, but are freely available and can be adapted by anybody for their specific needs. Examples include templates by Edinburgh Business School,<sup>399</sup> the University of the West of England,<sup>400</sup> Imperial College, London<sup>401</sup> and London's Global University,<sup>402</sup> and the Code of Conduct and the DPIA template<sup>403</sup> by the Family Links Network. Moreover, only a few projects have been funded specifically to create tools for the support of the DPIA process: namely, the Digital Data Protection Impact Assessment (DPIA) tool<sup>404</sup> and the Data Protection Impact Assessment (DPIA) Tool for Practical Use in Companies and Public Administration.<sup>405</sup>

A greater analysis and comparison of the tools available to be used for performing a DPIA, is depicted in D3.11, section 3.1.1 *Data Protection Impact Assessment Templates* [Sforzin 2020].

## 8.6.2 SWOT Analysis

Figure 20 shows the SWOT analysis performed for the medical data exchange demonstrator.

<sup>395</sup> [https://edpb.europa.eu/about-edpb/board/members\\_en](https://edpb.europa.eu/about-edpb/board/members_en)

<sup>396</sup> <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>

<sup>397</sup> <https://www.enisa.europa.eu/risk-level-tool/>

<sup>398</sup> <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment>

<sup>399</sup> <https://www.hw.ac.uk/documents/privacy-bydesign-dpia-toolkit.pdf>

<sup>400</sup> <https://www.uwe.ac.uk/about/structure-and-governance/data-protection/data-protection-impact-assesment>

<sup>401</sup> <https://www.imperial.ac.uk/admin-services/secretariat/information-governance/data-protection/processing-personal-data/data-assessments/>

<sup>402</sup> <https://www.ucl.ac.uk/data-protection/guidance-staff-students-and-researchers/practical-data-protection-guidance-notices/data-protection#download>

<sup>403</sup> <https://iapp.org/resources/article/template-for-data-protection-impact-assessment-dpia/>

<sup>404</sup> <https://localdigital.gov.uk/funded-project/digital-data-protection-impact-assessment-dpia-tool/>

<sup>405</sup> <https://www.dsfa.eu/index.php/en/home-en/>



Figure 20: Medical Data Exchange SWOT

### 8.6.2.1 Strengths

- In the EU, there exists a strong legal data framework to create trust and encourage data sharing **Data Governance Act**: Creation of data spaces, including the health sector, to enable at scale the exchange of data;
- **Data Protection**: There are strong data protection, privacy and cross-border operability regulations within the EU that rule the exchange of personal and sensitive data, including medical data (GDPR). This ensures the accountability of anybody mistreating such vital and personal data and, in turn, gives EU citizens the assurance of responsible management of their private data;
- **Mechanism for creating trust**: the commission supports the eIDAS authentication mechanisms, which increase the level of trust and security on data platforms. The eIDAS is connected to similar

national mechanisms (example: FranceConnect), enabling the creation of a large interconnected ecosystem of secured and trusted platforms, where participants are carefully vetted and identified.

### 8.6.2.2 Weaknesses

- Lack of sovereign trusted platforms for the exchange of medical data;
- Lack of support from EU partners and services: The Support **Centre for Data Sharing**, funded by the EC, has promoted Google solutions to share medical data<sup>406</sup>;
- Lack of homogeneity in health data legislations: while strong regulation on data protection, privacy and cross-border operability is one of the strengths, the regulations may, nonetheless, cause some adverse effects that can be seen as weaknesses. Strong regulation can introduce the problem of different interpretations of requirements and differences in related implementation costs, possible additional work for companies doing business in the EU (as compared with the rest of the world) and a higher entry cost or upfront cost, which is especially detrimental for new businesses.

### 8.6.2.3 Opportunities

- EU data strategy for the creation of data spaces, including the health sector;
- Rise of blockchain technology: increase trust, security, and transparency;
- Lessons learned from the COVID-19 crisis: health data sharing is key to fighting worldwide pandemics;
- Support from worldwide policy makers and institutions: European Commission, OMS, WEF.<sup>407</sup>
- COVID-19: The WHO and UNCTAD call for global health data sharing in order to prevent future pandemics.<sup>408</sup>

### 8.6.2.4 Threats

- Risk of GAFAM monopoly (Google, Amazon, Facebook, Apple and Microsoft): GAFAM are working to provide their technologies for the sharing of health data (*In France, the Health Data Hub is hosted on Microsoft*). Regarding the latest announcements of the commission (Data Governance Act, Digital Service Act), this is a major risk that Europe has to mitigate.
- Loss of sovereignty: Britain gave Palantir access to sensitive medical records of COVID-19 patients in a £1 deal<sup>409</sup>.
- Lack of trust from citizens.

## 8.6.3 European Digital Sovereignty

Data protection is one of the main aspects the European Union (EU) strategy is supporting, in order to recover “**digital sovereignty**”. This objective implies increasing the autonomy in the digital area by

<sup>406</sup> <https://eudatasharing.eu/fr/node/392>

<sup>407</sup> <https://www.covid19-dataexchange.org/resources>

<sup>408</sup> <https://unctad.org/news/unctad-calls-countries-make-digital-data-flow-benefit-all>

<sup>409</sup> <https://www.cnn.com/2020/06/08/palantir-nhs-covid-19-data.html>

developing actions and supporting initiatives that help citizens and companies in Europe achieve this end<sup>410</sup>. Given the huge growth of the data volume during the coming years in the EU (according to the EC forecast from 33 zettabytes in 2018 to 175 zettabytes in 2025, which means more than 800 billion € that year<sup>411</sup>), the creation of a single European data market will help public bodies, research organizations, companies and even citizens to adopt better decisions.

The creation of a European Health Data Space is one of the priorities of the Commission, as announced in the EU Data Strategy presented in February 2020. A common European Health Data Space will promote better exchange and access to different types of health data (electronic health records, genomics data, data from patient registries etc.), not only to support healthcare delivery (so-called primary use of data) but also for health research and health policy making purposes.

The entire data system will be built on transparent foundations that fully protect citizens' data and reinforce the portability of their health data, as stated in article 20 of the General Data Protection Regulation.

The Commission, in collaboration with the Member States, is engaged in the preparatory work and development of the European Health Data Space.

The European Health Data Space will be built on 3 main pillars:

- a strong system of data governance and rules for data exchange;
- data quality;
- strong infrastructure and interoperability.

The healthcare domain is one of the strategic sectors for boosting the data economy, creating an EU data framework that will allow secure access to data, preserving the user's data privacy when sensitive data are shared. The digital agenda supported by the EC through the Europe 2020 objectives has a real impact on the health domain, in order to improve EU citizens' health, increase the quality of care and reduce the health budget<sup>412</sup>. Towards this end, the use of health records by health bodies and medical data-sharing between parties involved in prevention and health care is required for EU citizens' health. As a consequence of the COVID-19 crisis, which has promoted remote healthcare and online medical data exchange, there is an emerging necessity for boosting digitalization in the health domain in Europe. Control of the data analysis related to the progress of infection, potential infection risks, and clinical trials for finding treatments and vaccines is required for developing measures and strategies for fighting against the Sars-Cov-2 virus. The risk of non-EU companies taking control of these kind of data could diminish EU Member States' sovereignty<sup>413</sup>.

The lessons learnt during the development of the medical data exchange demonstrator and the use of the indicated privacy-preserving technologies will help address the forthcoming challenges, not only in the health domain but also in other related business domains.

---

<sup>410</sup> [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS\\_BRI\(2020\)651992\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf)

<sup>411</sup> [https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en)

<sup>412</sup> [https://ec.europa.eu/health/europe\\_2020\\_en](https://ec.europa.eu/health/europe_2020_en)

<sup>413</sup> [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS\\_BRI\(2020\)651992\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf)

By defining standards for the exchange of medical data, the pilot will help the Commission to make the EU health data space possible. The pilot will bring proof that data exchange in the health sector can be carried out at the highest levels of security, and using only the solutions developed by EU players.

The pilot will act as living proof of an infrastructure at European level that could follow the overarching strategy of the European Data Space.

In this context, the Medical Data Exchange demonstrator is providing privacy-preserving tools, such as the DANS anonymization asset, to the COVID-19 Exchange platform. Additionally, during the following iteration of this demonstrator, strong authentication mechanisms for accessing the exchange platform will be provided. These actions, performed by European companies and organizations during the development of the CyberSec4Europe project, granted by the H2020 programme, will help to increase European digital sovereignty in the healthcare sector.

#### **8.6.4 COVID-19 and Public Health Dimension**

This section demonstrates how the medical data exchange demonstrator has been adapted to face the challenges generated by the COVID-19 pandemic, followed by some interoperability and privacy aspects related to the contact-tracing mobile apps developed by different countries.

##### **8.6.4.1 Medical Data Exchange demonstrator facing COVID-19**

Since the beginning of the COVID-19 crisis, health organizations across the world, backed by the World Health Organisation<sup>414</sup>, have started to investigate the causes behind the development of the virus in order to curb it.

Under emergency conditions, like those we are currently facing in Europe and globally due to the COVID-19 disease, the importance of medical data exchange becomes especially pronounced. With the pandemic putting immense stress on healthcare systems, efficient information gathering and dispensing of test results and directions in case of infection (while ensuring the privacy of those involved) have become very important. In addition to all of these, correct and efficient medical data exchange can reduce the work for healthcare workers and is especially welcome in times like these, when physical contacts (even with healthcare providers, when not absolutely necessary) are best kept to a minimum. During such emergency conditions, the possibility of an attack on a healthcare system, as well as the consequences of such an attack, drastically increase. In turn, the importance of secure and robust medical data exchange also becomes more relevant.

Aiming to overcome these challenges, facilitate the access to data, combined with the coordinated effort of all economic stakeholders at public and private level worldwide, is key to winning this war against the virus. Additionally, to hasten the resolution of this unprecedented global health crisis and mitigate the economic

---

<sup>414</sup> [www.who.int](http://www.who.int)

fallout and the repercussions on all businesses, data must circulate between organizations easily, securely, and extremely rapidly.

- The use of the COVID-19 Data Exchange platform for the pilot will help achieve the following goals:
- Scientific communities will be able to access vast amounts of data from all around the world, including data sources that are not easily available.
- Hospitals and other healthcare operations will have access to sophisticated yet easy-to-use tools to publish and share field data with the community.
- Many other stakeholders who have a direct impact on the resolution of this crisis will also be able to find or share valuable data. These include specialized equipment manufacturers and distributors, governmental agencies or public services.
- Strict confidentiality of the data exchanges will be enforced on the platform, where only carefully vetted participants will be authorized.
- Various types of data will be exchanged, including, but not limited to, statistical data, research data, anonymized raw data, test results and all types of other data (open data or commercial data)

More resources explaining the importance of data sharing are provided on the COVID-19 website<sup>415</sup>

#### 8.6.4.2 Mobile contact tracing apps in Europe

A powerful strategy for diminishing the transmission of COVID-19 between citizens is the creation of mobile contact-tracing apps that governments across the world have been developing during the last months. In the case of the EU, several tracking apps have been delivered<sup>416</sup> for breaking the chain of COVID-19 infections.

Different technical approaches have been followed by the countries for implementing these tracing apps. Table 7 shows some EU apps used by specific countries and evaluates them in terms of interoperability.

Table 7: Interoperability of mobile contact tracing apps in some EU Member States<sup>417</sup>

COUNTRY	APP	INTEROPERABLE	ABLE TO TALK TO ANOTHER APP
Austria	Stopp Corona App	Yes	No
Belgium	Coronalert	Yes	No
Denmark	Smitttestop	Yes	Yes
France	TousAntiCOVID	No	No
Germany	Corona-Warn-App	Yes	Yes
Ireland	COVID Tracker	Yes	Yes
Italy	Immuni	Yes	Yes
Slovenia	#OstaniZdrav	Yes	No

<sup>415</sup> <https://www.covid19-dataexchange.org/resources>

<sup>416</sup> [https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states\\_en](https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en)

<sup>417</sup> <https://www.covid19-dataexchange.org/resources>

Spain	Radar COVID	Yes	Yes
-------	-------------	-----	-----

In order to leverage the effort made by the EU Member States, the EC has launched an EU interoperability gateway<sup>418</sup> for linking tracing apps across Europe. Initially, three countries are involved: Germany, Ireland and Italy. The more countries that are linked to this system, the better tracing for cross-border mobility will be performed. Additionally, as many citizens download the national tracing apps, greater control over the pandemic can be achieved.

Some details of the German, French and the Spanish tracking apps launched by the three governments are provided in Table 8.

Table 8: Interoperability of mobile contact tracing apps in some EU Member States<sup>419</sup>

	<b>Corona-Warn-App</b> <sup>420</sup>	<b>TousAntiCovid</b> <sup>421</sup>	<b>Radar Covid app</b> <sup>422</sup>
Country	<b>Germany</b> (Robert Koch Institute-German national public health institute)	France	Spain
Open source	Yes	Yes	Yes
Third countries	Slovenia (#OstaniZdrav <sup>423</sup> )	No	No
Voluntary	Yes	Yes	Yes
GDPR compliant	Yes	Yes	Yes
Technology	Bluetooth & Apple/Google Exposure Notification APIs	Bluetooth	Bluetooth
Anonymous Random IDs	Yes	Yes	Yes
Minimum exposure time	10'	15'	15'
Personal identity data compile: name, surname	No	No	No

<sup>418</sup> [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_20\\_1904](https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1904)

<sup>419</sup> <https://www.covid19-dataexchange.org/resources>

<sup>420</sup> <https://www.coronawarn.app>

<sup>421</sup> <https://www.gouvernement.fr/info-coronavirus/tousanticovid>

<sup>422</sup> <https://radarcovid.gob.es/>

<sup>423</sup> <https://play.google.com/store/apps/details?id=si.gov.ostanizdrav>

address telephone number or email, geolocalization, tracking movements.			
Personal identity data delivery	No	No	No
Random Id mobile storage time	14 days	14 days	14 days
COVID-19 Positive code server storage time	14 days	14 days	14 days
Communicate COVID-19 test positive	Yes, by using secret QR code	Yes, by using single-use code or QR code.	Yes, by using a secret anonymous code.
Risk notification	Yes, on device. Based on the received data, the user devices match stored IDs and calculate the risk of infection based on the associated duration of contact and the distance to the other device.	Yes. The application will periodically query the server to see if any of its credentials have been returned by someone diagnosed or tested for COVID-19.	A notification is sent to all the devices holding the user's anonymous random ID. Therefore, these people are able to take appropriate preventive measures.
Decentralized approach	Yes	No	Yes
User privacy guarantee	Servers only hold (i) some anonymized data used to send verification keys and transaction numbers to ensure that the system works securely, and (ii) some pseudo-anonymized data (IDs)	The smartphones exchange, with each other and with the central server, pseudonymous identifiers that are specific to them. CNIL considered that the use of pseudonymous identifiers minimizes the possibilities of identification of the persons concerned	The mechanism developed by the Radar Covid system preserves the privacy of the user and the people around, as it does not identify either the user or the person she/he has been in contact with, nor does it collect any user location information.  The data stored in the mobile phone are cyphered.  The Radar Covid app does not share or sell data to third parties. The purpose of the stored information is only for controlling COVID-19 transmission.

Secure connection mobile-server	Yes	Yes	Yes. Secure and cyphered connections are established between the app and the server
---------------------------------	-----	-----	---

Basically, all of them works in a similar way. These tracking apps use Bluetooth technology to automatically detect and trace COVID-19 contacts. The apps exchange an anonymous random ID (after being 10-15 minutes in contact with another person under a social distance less of 2 meters), without sharing any personal data or positions. The smart phone will keep this anonymous IDs for 14 days. If a user has been infected, the health system delivers to the user an anonymous code which can voluntarily enter on the app, after a COVID-19 test confirming this situation has been performed. Then, people in contact with the infected person is automatically informed. Therefore, these people are able to take the appropriate preventing measures, limiting contact with other and contacting with the health service.

Despite the efforts invested by the governments developing these apps for effectively helping to fight against the COVID-19 transmission between the population. the degree of success in Europe was not the expected. The main reasons for this poor situation could be summarized in the following points<sup>424</sup>:

- **Number of users.** The efficiency depends on the number of **engaged users** using the tracing apps, as much citizens use these apps, the more possibility to detect and control the pandemic. Unfortunately, the number of downloads of these apps by the population was not the expected. Considering the countries indicated above a rough estimation<sup>425</sup> (between August and September) of the number of downloads and the adoption of the tracing apps range from 17,8 million times (22% of population) in Germany, 2,3 million times (4% of population) in France or 3,5 million times (7,6% of population) in Spain;
- **Efficiency.** According to the Harvard Business Review report<sup>426</sup> is needed a 60% of engaged population for stopping dissemination of the pandemic **effectively**;
- **Privacy issues.** Some concerns regarding the privacy of the underpinning technologies provided by Google and Apple arose from the first moment. Additionally, controversy between a centralized or decentralized model is ongoing. In a centralized model the data are uploaded to a server for matching the contacts allowing the server to learn about the data. In the case of a decentralized model the user has the control on their data stored in their own device, where the matching is made.
- **Willingness of tracing apps use.** The use of the tracing apps is voluntary in European countries while is compulsory in other countries like China. This political decision also affects the effectivity of the adopted measures;
- **The tracing apps adoption process.** The strategy for launching the tracing apps could also affect the user engagement. On the one hand the European countries decided to launch the tracing apps to all population waiting for a quick adoption of the solution, but on the other hand some experts

<sup>424</sup> <https://www.beckershospitalreview.com/healthcare-information-technology/why-contact-tracing-apps-fail-it-experts-share-5-reasons.html>

<sup>425</sup> <https://www.thelocal.com/20200909/do-any-of-europes-coronavirus-phone-apps-actually-work>

<sup>426</sup> <https://hbr.org/2020/07/how-to-get-people-to-actually-use-contact-tracing-apps>

recommend to address small target groups which can adopt the solution easily and then scale it to a big audience.

During the last months, knowledge, tools, techniques, methods and strategies has been adopted in order to avoid the spreading of the COVID-19. Is time to reflect and learn from the overall experience, based on the lessons learnt, for planning and develop a better strategy for stopping the dissemination of the virus.

Now, towards the end of 2021, we have a better understanding of the acceptance and effect of using contact tracing apps for COVID-19. And the unfortunate truth is that contact-tracing apps do not seem to have been much help in stopping or slowing it. At least some part of this can be attributed to the fact that its use never reached the critical mass that was estimated to be necessary for the apps to become effective [HPNK+ 2020] [BZA 2021]. The apps never caught on with users. There were many reasons why, including the questions surrounding privacy, the effectiveness of the solutions, technical difficulties and limitations, etc. [BZA 2021] [RCD+ 2021] [Singer 2021]. With the introduction of vaccines and because the tracing apps are not designed to take into account mitigation factors for contracting COVID-19 (such as vaccination, wearing masks or being outside) the apps fell out of favour.

### 8.6.5 Green Deal and Climate Change

One of the European Commission`s (EC) priorities is to achieve a “European Green Deal”<sup>427</sup> for overcoming the climate change challenge. The EC’s main goals for transforming the EU economy are to reach zero net emissions of greenhouses gases by 2050 and an economic growth decoupled from resource use. In this context digital technologies can support the decarbonisation of the economy.<sup>428</sup> It is estimated that around 1% of the total global electricity demand is consumed by data centres [Jones 2018], and a 15-30% increase in the energy consumption due to these activities is expected by 2030 [KK 2019].

The technologies involved in the data management domain, and the number of actors, use-cases, type of data and processes involved for data sharing are continuously growing, which leads to an important increase of consumption of energy [HH 2019]. Data centres use hardware (servers) and software solutions for managing a large amount of data, and the energy is used for processing and storing data, communicating (incoming and outgoing data flows) and cooling servers.<sup>429</sup> Additionally, the high-power demand of the technologies involved, such as AI/ML, DataOps or Blockchain, among others, implies an increase in carbon emissions and an environmental impact. Examples of high-power demand are the mining activity for getting cryptocurrencies (e.g. bitcoin), or training an advanced AI model.<sup>430</sup>

Data centres must be sustainable in terms of efficiency and use of clean energy sources. Some solutions are envisaged<sup>431</sup>:

- Develop high-performance cooling systems;
- Create efficient and automated data centre infrastructure management;

---

<sup>427</sup> [https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_en)

<sup>428</sup> [https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal/industry-and-green-deal\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal/industry-and-green-deal_en)

<sup>429</sup> <https://energyinnovation.org/2020/03/17/how-much-energy-do-data-centers-really-use/>

<sup>430</sup> <https://searchenterpriseai.techtarget.com/feature/Energy-consumption-of-AI-poses-environmental-problems>

<sup>431</sup> <https://dmexco.com/stories/green-data-centers/#uc-corner-modal-show>

- Expand the hardware lifecycle and promote the recycling of hardware.

Research is needed into energy consumption, reuse of the waste heat of data processing, and the efficiency of the implemented algorithms for managing data.

### **8.6.6 Impact on Democracy**

Medical data exchange does not have a direct impact on democracy. However, the COVID-19 pandemic has shown how a health crisis can start to unravel some aspects of civil society. Here we are primarily referring to the spread of health misinformation and conspiracies, sometimes culminating in large protests, low vaccination rates, etc. Additionally, there is also social injustice that can spread during such times. Medical data exchange is not a solution that would remove all of these problems; however, it can help to reduce them. It can give some semblance of transparency to boost the population's trust in health officials and the protective measures they are proposing or mandating. It can also potentially provide access to independent organizations that can help find new solutions and verify reported data and related findings.

### **8.6.7 Contributions to the EU CyberSecurity Strategy for the Digital Decade**

#### **8.6.7.1 Resilient infrastructure and critical services**

The technology used for the Medical Data Exchange demonstrator is cloud-native and based on a microservices architecture. It is designed to be cloud-provider agnostic. As such, it relies on standard managed services and can be deployed on any standard cloud provider.

The technology is deployed on a client's dedicated tenant and in the cloud provider and region of its choice, for facilitating compliance with national and local legislations.

This technology is designed for scalability. All core components of the application are stateless and can be scaled to multiple instances on demand, served by load balancers. Services are automatically spread among distinct availability zones, and their deployments are automatically orchestrated (through Kubernetes).

Databases are replicated in clusters. Master and replicas are spread among distinct availability zones. Multi-location data storage with replication is available. This technology provides both horizontal and vertical scalability.

- Global Cloud resources are automatically spread among distinct availability zones, including storage, load-balancers, VPCs and database services.
- All microservices use replication with AZ and blue/green deployment to handle a zero-downtime strategy.
- Stateful services running inside Kubernetes, like Elasticsearch and MongoDB, are deployed with a minimum of 3 members replica sets, also spread among multiple AZs.

Network capabilities and capacity are monitored and managed with advanced monitoring tools, allowing auto-scaling of resources based on usage variations.

#### **8.6.7.2 Building a European Cyber Shield**

The technology used for the medical data exchange demonstrator has obtained System and Organization Control (SOC) 2 Type I and SOC 3 certification. The completion of these examinations ensures the highest quality and security of services delivered are respected.

SOC 2 Type I and SOC 3 are standards guaranteeing the implementation of internal controls for security, availability, processing integrity, confidentiality or privacy. It also assesses and certifies the design of security processes and controls conducted by the organization.

Furthermore, regular audits (penetration tests) are conducted by security experts on the technology used and its code. No critical vulnerabilities were ever found. All vulnerabilities have been closed within the timeframe of audits.

### 8.6.7.3 An ultra-secure communication infrastructure

Multiple technical and legal security measures to ensure the protection of the personal data of the participants in the platform and those contained in the files exchanged on the platform are implemented.

**Data providers' and acquirers' responsibilities:** The COVID-19 Data Exchange Platform relies on principles of trust, security, responsibility and accountability. Each participant in its platform has to accept these terms of service to be part of the client's platform and to use it. Legal disclaimers and reminders of regulatory requirements are integrated along the user journey in the platform, including mandatory acceptance or confirmation action required from the participant.

**Location of data escrow:** The solution allows each data provider to choose on which cloud provider and in which region of the world (among those proposed on the platform by the orchestrator) they prefer to store the files until the data transaction is proceeded.

#### **Data offering including personal data configuration:**

- Legal disclaimers for both data providers and data acquirers
- Declaration of the country where the personal data were collected and processed to determine the regulations concerned (if this regulation is not currently managed as part of the solution or accepted by the orchestrator, the data are refused).
- Mandatory information such as: types of data, types of people, purpose of use, ...
- License restrictions

**License:** The Data Exchange Platform offers the support of three kinds of licenses:

- Personal data exchanged are blocked for data under open data licenses.
- When the data provider exchanges data with a standard and already existing license, it is his responsibility to integrate the necessary contractual provisions, according to the regulations to which the data are subject.
- For configurable licenses, the configurable license framework embedded in the solution integrates contractual clauses to inform the data acquirer of the conditions of use restriction on the data involved in the transaction, depending on the regulations to which the data are subject.

### 8.6.7.4 Securing the next generation of broadband mobile networks

This vertical does not directly contribute to this dimension.

#### **8.6.7.5 An Internet of Secure Things**

This vertical does not directly contribute to this dimension.

#### **8.6.7.6 Greater global Internet security**

This vertical does not directly contribute to this dimension.

#### **8.6.7.7 A reinforced presence in the technology supply chain**

This vertical does not directly contribute to this dimension.

#### **8.6.7.8 A Cyber-skilled EU workforce**

This vertical does not directly contribute to this dimension.

#### **8.6.7.9 EU leadership on standards, norms and frameworks in cyberspace**

This vertical does not directly contribute to this dimension.

#### **8.6.7.10 Cooperation with partners and the multi-stakeholder community**

This vertical does not directly contribute to this dimension.

#### **8.6.7.11 Strengthening global capacities to increase global resilience**

This vertical does not directly contribute to this dimension.

### **8.6.8 Sector-specific Dimensions**

The exchange of medical data involves several dimensions in the healthcare sector<sup>432</sup>, namely the hospitals and the private clinics from the health care dimension, and the wellbeing devices companies from the e/m Health dimension, which can play the role of data providers to the medical exchange platforms. The pharmaceutical industry and the medical devices industrial sector can also participate as consumers of the data shared on the exchange platforms. Besides these actors, research organizations and public health administrations can also play the role of data consumers.

Considering the public health domain where this demonstrator is located, as an extension to the ways medical data exchange can be used in facing COVID-19 (Section 8.6.4.1), it can also be used in improving the treatment, research and accessibility of medical data relating to any other ailments, conditions, etc. The demonstrator of medical data exchange in the project is geared towards COVID-19; however, the methodology of data collection and the technology of anonymization and protection can be applied to any other health data. A system with proven protection of privacy could increase the collection of data by reassuring the data subjects that they will not be individually exposed. Such solutions would also aggregate data from a wider space, again resulting in more data with better diversity (not based on data from a single hospital or country). Finally, and arguably most importantly, this would increase the accessibility of medical data. For those already working with them, it would only mean access to more data, but this would also

---

<sup>432</sup> [https://publications.jrc.ec.europa.eu/repository/bitstream/JRC111441/taxonomy\\_final.pdf](https://publications.jrc.ec.europa.eu/repository/bitstream/JRC111441/taxonomy_final.pdf)

encourage independent organizations, as well as organizations that may not generally work on medical data, but have some other expertise to further and collaborate on medical/public health research. An efficient, secure, and private medical data exchange could, therefore, significantly contribute to the area of public health.

### 8.6.9 Summary of the dimensions and impact on the Roadmap

The content provided in previous sections is related to several dimensions that affect the medical data exchange demonstrator. Given the sensitive data that are managed in the health domain, and the steadily growing amount of health data, the need for protecting this type of data and preserving data privacy is a basic goal. The use of tools for preserving user data privacy, assuring their integrity when stored and shared, is crucial. The aggregation of health data from patients and research studies, and their subsequent analysis, benefits doctors, health organizations and patients. In this way, the scheduled roadmap defined in this demonstrator has been focused on preserving data privacy, assuring the integrity of the data and providing strong authentication mechanisms for accessing the sensitive stored data. The use of anonymization and functional encryption tools, and the integration with the eIDAS network to use eID issued by EU Member States, are aligned with the fulfilment of Europe's regulations and their contribution to the European digital single market, while the underlying ideas regarding the described dimensions has been considered in the definition of the roadmap.

### 8.6.10 Challenge 1: Security and privacy

Medical data exchange market manages personal and sensitive data, a very special type of data that need to be secured. The lack of security measures will produce leak of this sensitive data with severe consequences.

#### Specific research goals

- **Protection of stored sensitive data.** The increase of stored sensitive data requires data protection measures must be put in place, guaranteeing the data protection at any moment. and.
- **Improve security measures for accessing sensitive data.** Data exchange platform users must be adequately identified. Only authorized persons can access to sensitive data., integrating security mechanisms and standards that protect against unauthorized access to the platform and prevent misuse of the data Continuous improvements in secure access are needed. Strong authentication for accessing data and innovative mechanisms for transaction tracking (e.g. blockchain) must be implemented.
- **Provide tools for securing data in transit.** Secure data exchange solutions must be built when sensitive data are transferred from the data producers to the data consumers, the security during the transference process must be assured.
- **Updating data exchange platforms.** On data sharing platform infrastructures, hardware and software updates must be applied regularly to avoid vulnerabilities that could be exploited by different attacks (e.g. data breaches, hacking, bugs, etc.).
- **Keep the integrity of the data.** Data loss or issues related to the integrity of the data can affect adequate patient evaluation and the procedures used to treat the patients. In this context, data integrity is needed during the course of a health treatment and the data must be managed in a privacy-preserving way by the data consumers (e.g. research institutions).

#### JRC Cybersecurity Domain:

- Data security and privacy

- Design, implementation, and operation of data management systems that include security and privacy functions
- Unlinkability
- Data usage control
- Identity and access management (IAM)
  - Identity management models, frameworks, services (e.g. identity federations)
  - Authentication/Access control technologies (X509 certificates, RFIDs, biometrics, PKI smart cards, SRAM PUF, etc.);
  - Protocols and frameworks for IAM
  - Identity management quality assurance
  - electronic IDentification, Authentication and trust Services (eIDAS)
  - Optical and electronic document security
- Software and Hardware Security Engineering
  - Security requirements engineering with emphasis on identity, privacy, accountability, and trust

#### JRC Sectorial Dimensions:

- Health

#### JRC Technologies and Use Cases Dimensions:

- Big data

### 8.6.11 Challenge 2: Mechanisms for preserving user data privacy

Due to medical data are stored and exchanged by different actors in this kind of platforms, the user data privacy must be guarantee at any moment, avoiding the misuse of these data, and in the case of leak the intruders can learn from them.

#### Specific research goals

- ***Keep the integrity of the data.*** Data loss or issues related to the integrity of the data can affect adequate patient evaluation and the procedures used to treat the patients. In this context, data integrity is needed during the course of a health treatment and the data must be managed in a privacy-preserving way by the data consumers (e.g. research institutions).
- ***Guarantee the privacy of the user data.*** The privacy of user data must be assured at any given moment; thus, technologies that allow for user data privacy, such as crypto technologies, must be applied. Even if the data are compromised, these technologies prevent the attacker from learning about the content of the data.

#### JRC Cybersecurity Domain:

- Data security and privacy
  - Privacy requirements for data management systems
  - Pseudonymity
  - Unlinkability
  - Privacy by design and Privacy Enhancing Technologies (PET)

#### JRC Sectorial Dimensions:

- Health

### JRC Technologies and Use Cases Dimensions:

- Big data

#### 8.6.12 Challenge 3: Trustworthiness on the data exchange platform

Security and privacy challenges are close linked with the **trust** challenges. A lack of security and privacy on data sharing platforms will affect directly the user's trust in this kind of platforms and is likely to decrease the willingness of citizens and patients to share health data. In this context, some controversies<sup>433</sup> may find expression in public opinion when public organizations launch initiatives to create data hubs for sharing health data.

#### Specific research goals

- **Increase the data subject confidence.** Some people are not willing to share their health data with third parties, neither for research purposes nor for commercial purposes on private sharing platforms. Basically, they have no trust in this kind of platform for reasons related to security and privacy.
- **Develop mechanisms for increasing data platform trustworthiness.** When an attack is suffered by a shared data platform, the confidence of data providers is lost, as their sensitive data are exposed and accessed without adequate control. In addition, the data consumers' confidence is affected as the integrity of the data is not guaranteed. In this scenario, research into activities, methods, tools and technologies that increase the confidence, transparency and trust in the sharing platforms must be developed. The lack of trustworthiness increases the number of people refusing consent to share data, and also reduces the number of transactions and the associated income.

### JRC Cybersecurity Domain:

- Trust Management, Assurance, and Accountability
  - Trust and privacy
  - Identity and trust management

### JRC Sectorial Dimensions:

- Health

### JRC Technologies and Use Cases Dimensions:

- Big data

#### 8.6.13 Challenge 4: Accomplish regulation during the data sharing process

Special consideration needs to be given to the **regulation** challenge, specifically those closely linked to privacy, that need to be treated with special attention since the EC push on this particular aspect. The following provides a more extensive description of this aspect, considering the main common points between the GDPR and the medical data sharing domain.

#### Specific research goals

- **Adopting the EU current regulation on data management.** Regulation (EU) 2016/679 of the European Parliament and the Council, more commonly known as the General Data Protection Regulation, is a legal framework that sets guidelines for the collection and processing of personal

---

<sup>433</sup> [https://www.thelancet.com/journals/landig/article/PIIS2589-7500\(19\)30163-3/fulltext](https://www.thelancet.com/journals/landig/article/PIIS2589-7500(19)30163-3/fulltext)

data. The healthcare sector is particularly affected, as GDPR defines stricter rules for processing of special types of data, which include data related to health.

Health-related, genetic and biometric data are under GDPR considered instances of sensitive personal data, which require a higher protection standard. Therefore, GDPR prohibits the processing of health-related data, genetic data and biometric data unless the data subject has given explicit consent, or when processing is necessary either for purposes of preventive or occupational medicine, or for reasons of public interest in the area of public health. One needs to study how the medical data sharing is affected by the GDPR.

- **Implement mechanisms for fulfilling the GDPR regulation.** Under the GDPR both the data controller and processor must implement appropriate technical and organizational measures (as will be described in deliverable 4.2 Legal Framework, in progress to be submitted in M12) to ensure a level of security appropriate to the risk. Management of risk also brings into consideration the Data Protection Impact Assessment (DPIA). DPIA is essentially a legally required (for certain situations) but more limited form of risk management. When processing health data, especially on a large scale, the DPIA is basically mandatory<sup>434</sup>. Failure to carry it out when required may result in a fine of up to €10 million, or 2% of global annual turnover if higher. Additionally, when processing health data both the controller and any processors have to appoint a Data Protection Officer (DPO), because (as stated in the regulation) this is necessary when the core activity consists of processing a special category of personal data on a large scale.

Relevant challenges to this include when and how to perform a DPIA and what is an appropriate level of protection, or how exactly should sensitive data be protected, to comply with the new regulation. Research on this regard are also needed.

- **Regulation implying cross-border transactions.** Regulation (EU) No 910/2014 of the European Parliament and the Council, dated 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market (more commonly known as eIDAS), is a fairly recent regulation that, as the name suggests, addresses electronic identification and trust services in the European single market. This ties in very strongly with health data exchange, which should transcend the borders of single member states to provide the best universal healthcare services across the EU.

Each of the member states was required to implement the EU Electronic Signature Directive into their national law. This caused two undesirable outcomes. In some cases, the local legislation was not produced in time to support the rollout of eIDAS. The freedom the regulation allowed to member states when they designed their own systems has also led to problems. Different member states have proposed and implemented different solutions that are not necessarily compatible between member states, thus defeating the principal idea behind eIDAS. Further, member states were left with the freedom to regulate their own measures in other areas of electronic commerce. This has led to a position where other regulations come into conflict with the eIDAS regulation, thus blocking further harmonization of the single European market.

---

<sup>434</sup> Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing ‘Is likely to result in a high risk’ for the purposes of Regulation 2016/679, 2017. Available at [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=611236](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236). Last accessed 13.11.2019.

- **Use of EU eID for cross-border transactions.** Services for medical data exchange require the authentication of parties included in the exchange. To facilitate the authentication across the EU, regardless of the country the parties exchanging the data are from, the use of an all-EU eID would help unify the experience and access across the EU. The challenge is, therefore, to find the current status of member states and to investigate the possibilities of using such an eID

#### JRC Cybersecurity Domain:

- Legal aspects

#### JRC Sectorial Dimensions:

- Health

#### JRC Technologies and Use Cases Dimensions:

- Big data

### 8.6.14 Challenge 5: Data exchange platform user experience

Apart from the challenges described above, which are mainly related to security, privacy and regulation, medical data sharing platforms also need to tackle the user experience.

#### Specific research goals

- **Improve user experience interacting with the sharing data platforms.** It is necessary to pay attention to the interaction between the user and the different processes and services offered by the platform. Additional user experience research is needed in order to increase the user's business engagement and to improve the user/consumer's perception of privacy and data integrity.

#### JRC Cybersecurity Domain:

- Human Aspects
  - Usability

#### JRC Sectorial Dimensions:

- Health

#### JRC Technologies and Use Cases Dimensions:

- Big data.

## 8.7 Mapping of the Challenges to the Big Picture

According to the description provided in section 8.1, the considered general aspects applied to the general data exchange domain can be mapped to the specific challenges identified in section 8.6. The medical data exchange platform must provide a secure access to the data, also keeping the integrity of the data when are stored or in transit (challenge 1). One of the main issues when personal and sensitive data, as health data, are sharing is the privacy matter. The platform will provide mechanisms for preserving the user data privacy (challenge 2). The adoption secure measures and the use of privacy preserving techniques will increase the trustworthiness in the exchange platform (challenge 3). The accomplish with the common European regulatory rules (GDPR), especially those related with privacy when sensitive data are shared, will facilitate the cross-border data exchange (challenge 4). Finally, the use of tools and technologies which are facilitating the user experience will increase the willingness to share data. (challenge 5).

## 8.8 Methods, Mechanisms, and Tools

According to the research challenges described in section 8.6, the medical data exchange demonstrator will address the described challenges using the following sources:

- Assets provided by Task 3.2 Research and Integration on Cybersecurity Enablers and underlying Technologies in WP3;
- Assets developed in the context of Task 5.6 Medical Data Exchange in WP5;
- Assets developed in other European projects that fit with the Medical Data Exchange demonstrator.
- Asset provided by Task 3.3 SDL-Software Development Lifecycle in WP3;
- Asset provided by Task 3.7 Regulatory Sources for citizen-friendly goals in WP3;

### 8.8.1 Challenge 1: Security tools

The protection of the sensitive data managed in Task 5.6 Medical Data Exchange and the access to the platform where these data are shared must be assured. To this end the following assets from WP3 will be used.

**Service Provider eIDAS integrator (SPeIDI).** This asset is intended for integrating digital services into the eIDAS network for authentication scenarios when strong user authentication is needed, securing access to those services. “Based on the building blocks provided by CEF, SPeIDI follows the eIDAS technical specifications, including signing, encryption and the SAML 2.0 standard” [Skarmeta 2019]. Its modular design allows a flexible integration with different SPs and protocols used by the MS eIDAS nodes. This asset will be updated in the context of T3.2 during the CyberSec4Europe project.

The SPeIDI asset was originally dedicated to integrating private service providers with the Spanish eIDAS node. As the final connection with the eIDAS network has been performed through the French eIDAS node, a module has been implemented for integrating the French eIDAS node managed by the French authorities. The FranceConnect<sup>435</sup> mechanism, based on eIDAS, has been integrated into the COVID-19 Data Exchange Platform, ensuring a more secure and smooth experience for the users.

**Self-Sovereign & Privacy-preserving (SS-PP-IdM).** This asset is envisaged to investigate, integrate and adapt privacy-preserving solutions, such as the anonymous credentials systems in blockchains, following a self-sovereign identity management approach. To this end, it is envisaged to use, as baseline, the outcomes from the Decentralized Identity Foundation (DIF) [Skarmeta 2019]. The assets will be aligned with “Verifiable Credentials” and “Decentralized Identifiers” (DIDs) standards from W3C. This asset is being developed in the context of T3.2 during the CyberSec4Europeproject.

The use of this asset in the Medical Data Exchange vertical will be limited to the analysis and the benefits of the adoption of this decentralized identity approach in the data-sharing marketplace domain.

---

<sup>435</sup> <https://franceconnect.gouv.fr/>

Data protection tools such as an encryption asset will be used and is described in section 8.8.2.

### 8.8.2 Challenge 2: Privacy-preserving assets

Privacy preserving techniques will also be used in order to preserve the user data privacy.

**Data Anonymization Service (DANS)**, is an “anonymization service that provides different privacy models (e.g. the k-anonymity model) to enable the application of certain privacy criteria over a specific dataset” [Skarmeta 2019]. DANS is intended to be integrated by data managers (data producers/aggregators) in scenarios where sensitive personal data is managed, such as big data analytics platforms, research projects or clinical trial data sharing, in order to prevent misuse of data and preserve users’ privacy. This asset will be developed in the context of T5.6 in WP5 during the CyberSec4Europe project.

**Functional Encryption to Medical Data (FE2MED)** “is an asset that provides an FE library containing attribute-based encryption schemes for the preservation of privacy in health information management” [Skarmeta 2019]. It is being developed under the umbrella of the FENTEC<sup>436</sup> EU project and is intended for users who provide health data, data providers and data consumers, in order to offer end-to-end data privacy.

Currently this encryption tool offers two encryption schemes:

- Attribute-based encryption (ABE) for sharing sensitive data;
- Inner product for sharing analytics results.

PLEAK is an “analysis tool for the privacy audit of an existing system and the design of new privacy-aware systems” [Skarmeta 2019]. The use of this asset by the Medical Data Exchange vertical will help to prevent privacy issues and facilitate the management of risks during data sharing, following the principle of privacy by design.

### 8.8.3 Challenge 3: Trust mechanisms

As indicated in section 8.6.12, the user willingness to share sensitive data in a Data Exchange Platform (DEP) is based on trust. For DEPs the trustworthiness is based on the implemented security mechanisms and the privacy-preserving measures the DEP applies on user data. In this context the described assets in sections 8.8.1 and 8.8.2 play a crucial role for providing security and privacy during the sensitive data exchange process.

### 8.8.4 Challenge 4: Accomplish Regulations

To help alleviate the challenges regarding the adoption of and compliance with the GDPR, Task 3.7 Regulatory Sources for citizen-friendly goals in WP3 of the CyberSec4Europe project proposes that guidelines should be established for a GDPR-compliant user experience. This document collected and presented a simple and understandable way the specific points of the GDPR regulation and suggested

<sup>436</sup> <http://fentec.eu/>

methods for achieving them, thus helping to overcome the previously mentioned challenges. The GDPR-compliant user experience is a solution that collects important interpretations of the regulation, together with good implementation examples, focus especially on how and when to perform a DPIA.

In addition, in Task 3.7, there will be research into the interoperability and cross-border compliance of the eIDAS between different countries. The main objective of this work is to find discrepancies between member states and possibly to identify the security shortcomings of a given authentication implementation.

### 8.8.5 Challenge 5: User Experience

Data visualization is a very popular feature and is often considered a prerequisite to data valorisation. Graphical representation is actually quite useful when exploring data, especially new data.

What is sometimes overlooked is the complexity of automatic data visualization. Being able to draw nice pictures from a dataset requires going through all the steps of data preparation, including data discovery, cleansing and formatting. Some of these steps might be partly automated, but fully automated data visualization from an unknown dataset is out of reach. For example, choosing the right columns to draw, when dealing with tabular data, is not something that can be easily automated.

Developing internal data preparation and visualization routines has been carefully considered. The implementation of such tools would be quite demanding and would require considerable efforts from the team.

Dawex has decided to proceed with improvements of the current data assessment and visualization tools:

- Heatmap
- Treemap
- Histogram
- Data types
- Data sampling automatically generated by the platform

These tools allow a smoother experience for the users, while not adding overly high costs and complexity to the platform. The next step will be to add a system of connectors, to allow the users to easily transfer the data acquired through the platform with a single click into the data analysis & science tools they use.

Additionally, Atos has designed a user interface (UI) for the DANS asset, being implemented at this moment. This UI will improve the user experience and facilitates the work of the anonymization tool users.

This maps the tools addressing the challenges identified in the Medical Data Exchange vertical.

Table 9: Challenges identified in the Medical Data Exchange Vertical and Tools needed to address them

Challenge	Tools required for	Tools contemplated for Medical Data Exchange	Tools/Methods that need to be addressed
-----------	--------------------	--	---

Challenge 1	Security tools	eIDAS connector (D3.1, Section 5.1), SS-PP IdM (D3.1, Section 5.1)	Secure shared data space infrastructure with access control
Challenge 2	Privacy-preserving assets	DANS (D3.1, Section 5.1), FE2MED (D3.1, Section 7), PLEAK (D3.1, Section 5.2)	Privacy preserving infrastructure
Challenge 3	Trust mechanisms	eIDAS connector (D3.1, Section 5.1), SS-PP IdM (D3.1, Section 5.1), DANS (D3.1, Section 5.1), FE2MED (D3.1, Section 7)	Trust in shared data space infrastructure
Challenge 4	Regulation accomplish	Guidelines for GDPR compliant user experience (D3.1, Section 5.6), and general-purpose	Adaptation data sharing scenarios
Challenge 5	User experience	DEP visualization tool and DANS UI developed in the context of T5.6 by Dawex and Atos respectively	Graphical representation and making easier the use of tools

## 8.9 Roadmap

### 8.9.1 Short-term plan

An analysis of the initiatives launched following the COVID-19 pandemic, aiming to facilitate better data circulation among the health stakeholders. A recent case study could be the initiative from the WHO, launched with the German government, to build a Data Hub.<sup>437</sup>

The WHO Hub, which is receiving an initial investment of US\$ 100 million from the Federal Republic of Germany, will harness broad and diverse partnerships across many professional disciplines, and will use the latest technology to link the data, tools and communities of practice so that actionable data and intelligence are shared for the common good.

The Hub will work to:

- Enhance methods for access to multiple data sources vital to generating signals and insights into disease emergence, evolution and impact;
- Develop state-of-the-art tools to process, analyse and model data for detection, assessment and response;
- Provide the WHO, our Member States and partners with these tools to underpin better, faster decisions on how to address outbreak signals and events; and
- Connect and catalyse institutions and networks developing disease outbreak solutions for the present and future.

The launched hub for pandemic and epidemic intelligence will become something very similar to the solution demonstrated in Medical Data Exchange in CyberSec4Europe (Task 5.6) and will have to, in some measure, address all the challenges discussed here (Sections **Error! Reference source not found.-Error! Re**

<sup>437</sup> <https://www.who.int/news/item/01-09-2021-who-germany-open-hub-for-pandemic-and-epidemic-intelligence-in-berlin>

**ference source not found.**) The case study produced in this project (shortly described in section 8.6.4.1 and presented in deliverable D5.4 [Sforzin 2021]) could provide the WHO with useful insights about what works and doesn't work in real conditions. Both solutions will provide different perspectives on the used approaches and conducted work for forthcoming solutions and inspire us and others for the future of the COVID-19 Data Exchange Platform and other medical data sharing solutions.

This case study could bring different perspectives to the work conducted in the medical demonstrators and inspire us for the future of the COVID-19 Data Exchange Platform. Using the lessons learned from the demonstrator, we could also provide the WHO with useful insights about what works and doesn't work in real conditions.

A study on the interoperability and cross-border compliance of eIDAS implementations, focusing on authentication mechanisms, will be finished shortly. It will provide information on possibilities for using the eIDAS network across the EU with the proposed medical data exchange solution.

Finally, the adoption is planned of user interfaces for privacy protecting assets aimed at facilitating the user experience.

## 8.9.2 Beyond the end of the project plan

### 8.9.2.1 Security 2025

Additional research activities need to be performed after the end of the project in order to address some gaps identified during the development of the medical data exchange demonstrator:

- A standard for health ontologies and metadata, allowing easier and more secure circulation of data;
- Adoption of advanced encryption technologies (homomorphic encryption);
- A stronger and harmonized legal framework for licensing contracts that cover the exchange of health data
- Encouraging medical professionals to use encryption in healthcare;
- Use of more secure data storage services in hospitals;

Definition of European guidelines and principles for the creation of data warehouses (“entrepôts de la donnée”<sup>438</sup>) built by hospitals, to ensure the highest levels of security.

### 8.9.2.2 Security 2030

The growth of the healthcare market is expected to be more than 25% in the coming years.<sup>439</sup> New challenges and threads will arise in the future, and the health domain needs to be ready to face them.

---

<sup>438</sup> <https://www.ticsante.com/story/4831/entrepots-de-donnees-de-sante-les-chu-pointent-un-besoin-de-confiance-et-de-competences.html>

<sup>439</sup> <https://www.marketwatch.com/press-release/healthcare-analytics-market-size-and-share-high-during-forecast-year-2030-2021-08-25>

In order to be prepared for these challenges, it is necessary to be aware of the technical initiatives being developed at this moment. Among these initiatives is the openEHR<sup>440</sup> (open Electronic Health Record) technology for e-health, which will “create standards and build information and interoperability solutions for the healthcare domain”.<sup>441</sup> The main benefits of this technology are that the implemented solutions are generated by the openEHR community (e.g. health professionals), and it facilitates computing health data, facilitating patient treatment and research. The adoption of this kind of open platform will allow rapid data sharing among hospitals/countries if a need arises, as evidenced by the COVID-19 pandemic. Additionally, these initiatives facilitate the integration of systems for sharing data for patient care and research purposes.

## Challenges

Another interesting aspect to be considered in the future is that of big data analytics tools. The adoption of AI/ML in the e-health domain for speeding diagnosis and helping find the right treatment<sup>442</sup> is already ongoing and will grow by around 38% by 2030.<sup>443</sup>

The need to provide better healthcare quality and a faster and more accurate diagnosis implies the management of a large amount of health data from devices, electronic health records, medical imaging and clinical trials or research. Compared to classical computing systems, quantum computing can reduce the calculation times from years to minutes.<sup>444</sup>

however, quantum computing also has security implications One of the big challenges the e-health domain is facing is to protect the user’s data privacy, particularly this type of sensitive data. Encryption mechanisms are used for preserving privacy and integrity. Since the calculation times can be reduced to minutes, the use of cryptographic mechanisms can be compromised by quantum computing.<sup>445</sup> More advances in the quantum field are expected in future years, related to DNA sequencing and analysis, drug design, simulated clinical trials, processing huge amounts of data from patient’s sensors in real time, facilitating doctors’ decision making, and creating stronger medical data systems.<sup>446</sup>

In summary, given the development of the big data it is necessary to work on updating and revising legal frameworks and ethical guidelines, as well as preserving-privacy solutions that will give a comprehensive answer to the forthcoming challenges and threats.<sup>447</sup>

### 8.9.3 Milestones

According to the roadmap described in previous deliverables [Markatos 2020] [Markatos 2021] the following milestones are expected to be reached at the end of the project:

---

<sup>440</sup> <https://www.openehr.org/>

<sup>441</sup> [https://www.openehr.org/about/what\\_is\\_openehr](https://www.openehr.org/about/what_is_openehr)

<sup>442</sup> <https://www.globenewswire.com/en/news-release/2021/09/30/2306203/0/en/Global-AI-in-Healthcare-Market-Size-to-Hit-194-4-Billion-By-2030-Allied-Market-Research.html>

<sup>443</sup> <https://www.alliedmarketresearch.com/artificial-intelligence-in-healthcare-market>

<sup>444</sup> <https://www.ibm.com/thought-leadership/institute-business-value/report/quantum-healthcare>

<sup>445</sup> <https://www.ibm.com/thought-leadership/institute-business-value/report/quantumsecurity>

<sup>446</sup> <https://medicalfuturist.com/quantum-computing-in-healthcare/>

<sup>447</sup> [https://www.unescap.org/sites/default/files/1\\_Big%20Data%202030%20Agenda\\_stock-taking%20report\\_25.01.16.pdf](https://www.unescap.org/sites/default/files/1_Big%20Data%202030%20Agenda_stock-taking%20report_25.01.16.pdf)

- DANS user interface implemented and tested
- FE2MED implemented and tested. User guide delivered
- eIDAS connector tested and validated
- Validation of visualization tool
- Adoption and validation of PLEAK asset
- Plan to validate the GDPR tool
- Analysis of benefits to medical data exchange demonstrator using the SS-PP IdM asset.

## 8.10 Summary

This section focused on user privacy protection when personal and sensitive data (such as medical data) are shared between parties. As explained in sections 8.1 and 8.2, some of the main challenges in the digital economy and particularly in the medical data exchange include: (i) preserving user privacy, (ii) assuring the secure access to data, and (iii) providing trusted environments where the data providers and data consumers can share sensitive data. Additionally, (i) assuring the end-to-end data integrity, (ii) improving the user experience, and (iii) applying innovative tools to comply with regulations (such as GDPR), will facilitate the broader use of the data sharing platforms among users. The envisaged mechanisms to be used will help to avoid the actions and/or mitigate the adverse effects of intruders (described in section 8.4). [Markatos 2021]

Section 8.6.1 describes the current status of the state of the art related to identity management and eIDs, medical data privacy and the legal and regulatory framework. Section 8.6.2 presents an updated SWOT analysis that shows the current situation of the medical data exchange domain in the EU, regarding user data sharing while preserving privacy, trustworthiness and security, and complying with regulations. It shows that homogeneity in health data EU regulation will help to facilitate the use of health records, which can, in turn, become a key factor for fighting against pandemics, while increasing the citizens' trust in any data exchange platforms used.

The COVID-19 crisis boosted the development of innovative tools for tracing and controlling the pandemic; however, as indicated in section 8.6.4, several aspects, such as privacy, security and strategy, must be considered in order to achieve the expected objectives.

Section 8.6.5 indicates how data exchange and in general data spaces can affect climate change.

Section 8.6.6 suggests how initiatives such as the COVID-19 Data Exchange platform can contribute to minimise the effect of fake news and improve cooperation.

Section 8.6.7 identifies those aspects the Medical Data Exchange demonstrator can contribute to the EU CyberSecurity Strategy for the Digital Decade.

Section 0 considers how this demonstrator is relevant to the health domain.

In this context several challenges are identified in section 8.7:

- Challenge 1: Security tools
- Challenge 2: Privacy-preserving assets
- Challenge 3: Trust mechanisms
- Challenge 4: Accomplish Regulations
- Challenge 5: User Experience
- Dealing with these challenges should be of high importance in the near future, as an increasing number of sensitive records are generated by the digital economy. Trusted data exchange platforms will increase European Digital Sovereignty, but they need to adopt new paradigms such as (i) self-sovereign identity, (ii) blockchain technology, and (iii) returning control of the data to individual users.

## 9 Smart Cities

### 9.1 The Big Picture

Today, an increasing number of people worldwide live and work in cities. Consequently, creating livable environments in which people and businesses can thrive has become one of today's most pressing issues: the way we all use the time and the space available, the environment and the resources at our disposal determines the quality of our life and forms the basis for the sustainability of our existence in the medium and long term<sup>448</sup>. For that reason, many cities and metropolitan areas are embracing the “Smart City” concept, that is adopting a more efficient management of services and turning cities into enablers of innovation, economic growth, and well-being, but also safe, dynamic and inclusive.

This transformation process needs all levels of government together with organizations and networks of cities and communities of all sizes, with strong cooperation through multi-level governance and co-creation with citizens. To do this, a first step is needed: the smart city (SC) enablers' adoption. The role of these enablers is to connect consumers and producers, enabling a federated publication of context data, allowing service providers to find and use data from city and third-party sources while preserving data sovereignty<sup>449</sup>.

Digital solutions, supported by locally generated data, are capable of providing high-quality services both to the public and to businesses. These solutions incorporate smart urban mobility, energy efficiency, sustainable housing, digital public services and civic-led governance. To receive public trust for such systems, data must be used responsibly via digital platforms, and their quality, security and privacy must be ensured<sup>450</sup>.

Specific processes need to be put in place to support this paradigm. The basic concept here is to collect data from many distributed sources, then perform data aggregation and analytics in order to extract meaningful information to drive decision processes. Data can be provided by official sensors as well as by citizens and entities willing to contribute information for the collective benefit (e.g. smartphone position for traffic estimation). Collected data can not only be used by local government but also be provided in open form, to permit direct usage by citizens, interest groups, or companies in innovative ways. Data collection and processing is at the core of the smart-city paradigm.

Various stakeholders are involved and they can be divided in four main groups: Users (of the goods and services), Drivers (that build sustainable solutions), Resource Providers (that perform research, drive innovation, and augment knowledge), and Framework Enablers (that create a vision, enable resources, and promote an environment for innovation). For example:

- Users - citizens, tourists, NGO's, public interest groups
- Drivers - technical, manufacturing, utility, consulting and business firms

---

<sup>448</sup> [https://www.eng.it/resources/whitepaper/doc/augmented-city/augmented-city-whitepaper-eng\\_.pdf](https://www.eng.it/resources/whitepaper/doc/augmented-city/augmented-city-whitepaper-eng_.pdf)

<sup>449</sup> <https://www.fiware.org/community/smart-cities/>

<sup>450</sup> <https://www.living-in.eu/declaration>

- Resource Providers - universities, urban planners, think tanks, and technical companies
- Framework Enablers - City councils, elected officials, standardization committees, and financial organizations

We can sketch a smart-city value chain with the following picture, to explain relations and dependencies between the stakeholders and the services (see Figure 21):

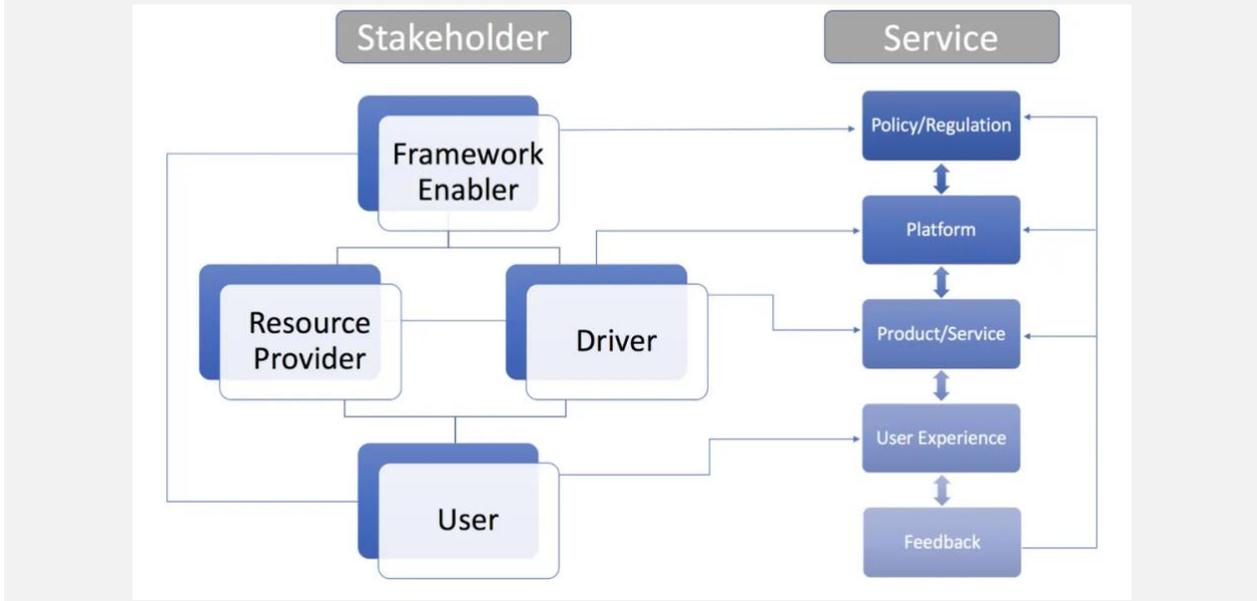


Figure 21: Stakeholders and services

Obviously, new smart services could bring new threats, therefore efficient risk management is needed, to better prevent and react to these new threats.

## 9.2 Overview

As a result of a significant increase in the number of interconnected devices, smart cities (SCs) are suffering an unprecedented attack surface. A SC<sup>451</sup> needs to be protected by a joint project involving the Local Public Administration (LPA) and the private sector.

First of all, what are smart objects? Except to experts, an “intelligent” traffic light might seem not so different from one that is not. However, developments in computational intelligence have allowed “intelligence” to expand beyond computers to other objects, allowing those objects to communicate with each other. Once this communication reaches a certain threshold, it opens up a new horizon of services, which are capable of improving the quality of citizens’ lives and work. Everything thus becomes smarter, more comfortable and more useful.

<sup>451</sup> SC stands for Smart City  
300

Of course, this is not an immediate process, a LPA must first equip itself with the necessary tools. The enabling architecture for introducing the IoT in the cities has four levels: infrastructure, sensors, service delivery and user applications:

- **Infrastructure:** a network capable of transporting and managing the enormous amount of information that has to move throughout the city.
- **Sensors:** a plethora of sensors (audio, video, proximity, temperature, air pollution, etc.) installed in public spaces, where they collect data on the environment, user behaviour and the infrastructure status (diagnostic sensors).
- **Service delivery:** this aims to collect data from an underlying layer and provide it to the next, reworking or adding/highlighting value where possible, in order to improve the services offered by the LPA that are currently available to citizens.
- **User applications:** these deal with the users' interaction, whether they are employees of the LPA (in charge of managing the services) or citizens (beneficiaries of the services offered by their city).

This last level will benefit from the information security features designed and demonstrated within the project.

### 9.3 What is at stake?

Within this section, the major research challenges are presented, starting with answering to corresponding questions, in order to give a clear context of the SC domain. A list of these research challenges can be found at the end of the section.

#### 9.3.1 What needs to be protected?

At a time when the physical world is converging on a digital one, there are several key factors that influence cyber risk in the context of a SC. These key factors include the integration between the digital and the physical environment, interoperability between legacy and new systems, and the integration of services through IoT and digital technologies.

From a SC point of view, the richly diverse variety of hardware devices and software elements first comes to mind as presenting serious security challenges. Starting from the most basic principles of security, **confidentiality, integrity and availability**, it is easy to recognize that hardware and software must provide sufficient protection not only to ensure the good functioning of the system itself, but also to avoid any loss of data that may have severe impact on the entire infrastructure. **From IoT devices**, through the communication hardware transporting information, to the cloud infrastructures acting as service providers, all steps are composed of different technologies with very different specifications and capabilities, and all of them must work together for the common goal of security.

Figure 10 gives a general idea of what are the most relevant components/assets in the SC context [CER 2019]. However, given the increasing adoption of smart technologies in physical infrastructures to create environmental and economic efficiencies, the associated risks are not well understood.

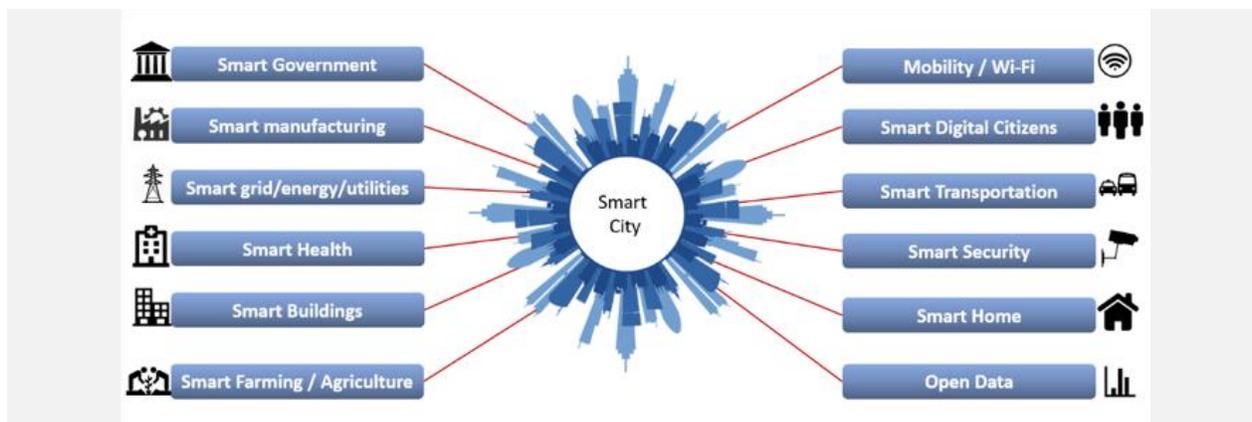


Figure 10: SC Stakeholders (Source: [CER 2019])

ENISA provides several white papers about **good practices for IoT and smart infrastructure tools**<sup>452</sup>, whose intent is to provide an aggregated view of the several studies that have been published in recent years. about smart cars, smart hospitals, smart airports, Industry 4.0 and SC. Such publications help to understand in detail what are the assets that need to be protected and what are the most dangerous threats.

Figure 11 shows the assets that need to be protected in an IoT ecosystem, while Figure 12, shows the asset taxonomy for Industry 4.0 [ENISA 2018].

ENISA defines IoT as “*a cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decision making*” [ENISA 2017], but it is also the case that there is growing social concern about **privacy and data protection**, as the human aspect of every IT system becomes increasingly predominant (see Figure 22 and Figure 23).

<sup>452</sup><https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool/results#IoT>

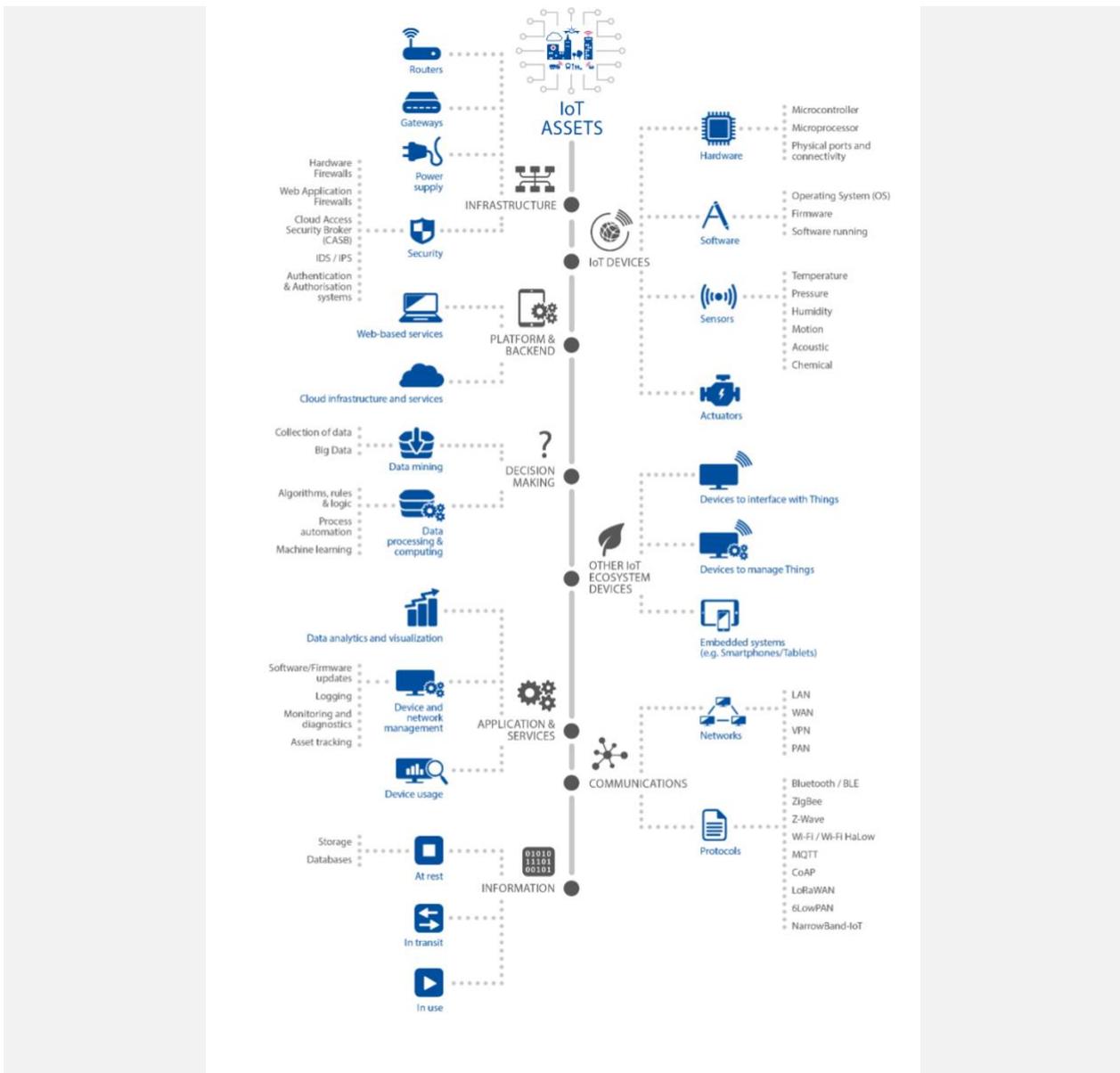


Figure 22: IoT Assembly Taxonomy (Source [ENISA 2018])

Regulations such as GDPR are an example of the scenarios that will have a direct impact, not only on how data is stored, but on many other related processes that directly impact on SCs.

More and more people are part of the system. Social initiatives, peer-to-peer services, asset sharing and a plethora of other use cases show that many aspects of society (economy, health and safety, learning, etc.) will strengthen their presence in the digital realm, creating a shear force between the availability of data and confidentiality that will be difficult to overcome.

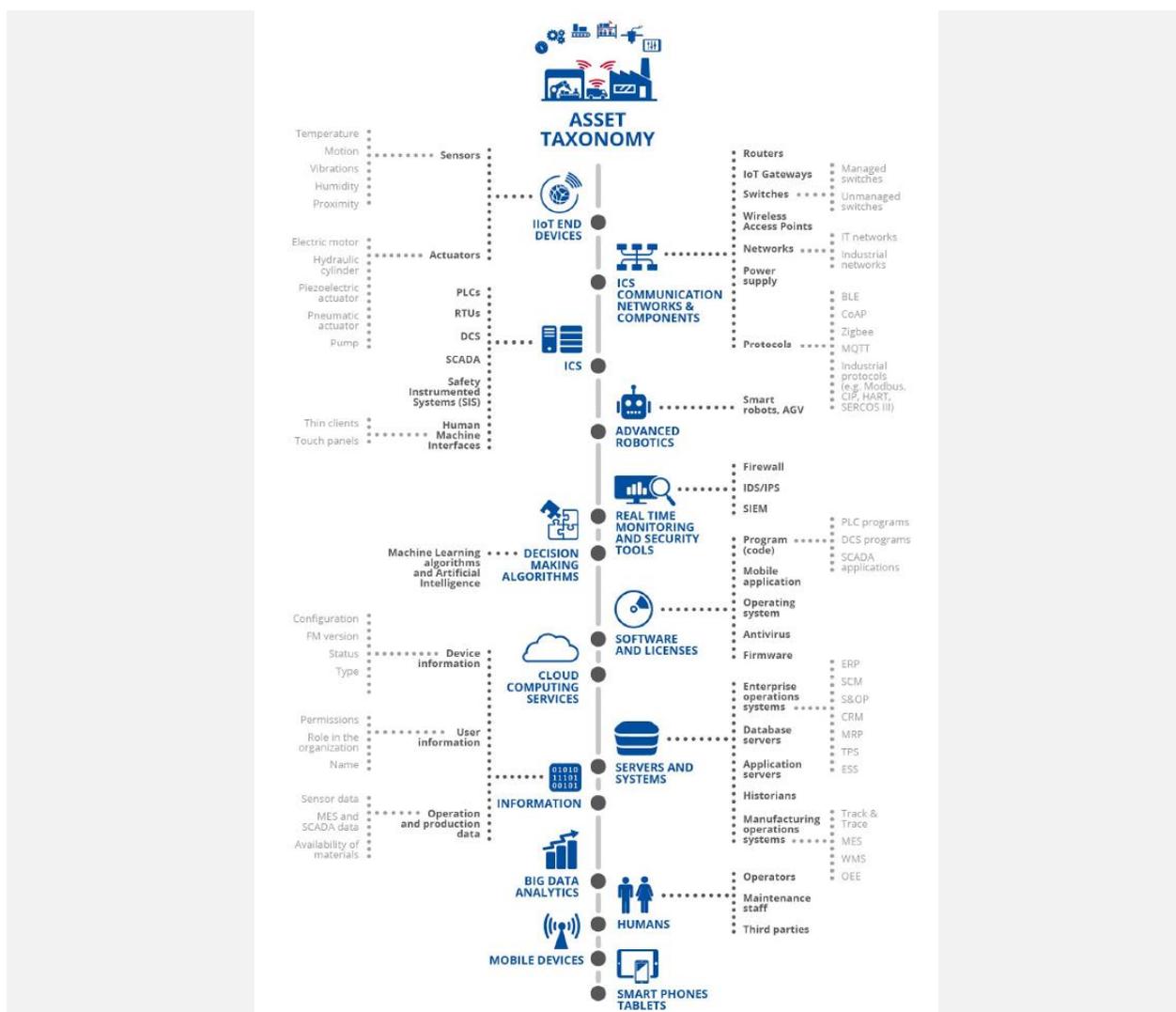


Figure 23: Industry 4.0 Asset Taxonomy (Source: [ENISA 2018])

### 9.3.2 What is expected to go wrong?

In SCs, the rise of the technology used to increase productivity and efficiency among both physical and digital infrastructures exposes a wide range of vulnerabilities that can be exploited by cyber criminals and other malicious or unwitting actors. SCs are vulnerable to a number of high-level threats that are associated with various problems of cyber security.

Smart traffic controls, smart parking, energy and water management, smart street lighting, public transportation and security are of greatest concern, since the unencrypted communication and lack of cyber security testing on IT systems allows hackers to manipulate and disrupt smart services. Of major concern are attacks on critical infrastructures, such as transportation, water or power systems [Seattle 2019].

Figure 24 illustrates the threat taxonomy identified by ENISA. Most of the potential threats are basically related to **privacy, data & identity theft, device hijacking, denial of service, application level distributed denial of service, and man-in-the-middle attacks and ransomware.**

**Man-in-the-middle<sup>453</sup>:** The attacker places himself in the communication channel between the two components. Whenever one component attempts to communicate with the other (data flow, authentication challenges, etc.), the data first goes to the attacker, who has the opportunity to observe or alter it, and is then passed on to the other component as if it had never been observed. For example, a man-in-the-middle attack on a smart valve can be used to deliberately cause wastewater overflow.

**Data & identity theft:** Data generated by unprotected infrastructure, such as parking garages, surveillance feeds and so on, provides cyber attackers with ample targeted personal information that can potentially be exploited for fraudulent transactions and identity theft.

**Device hijacking:** The attacker hijacks and effectively assumes control of a device. In the context of an SC, a cyber-criminal could exploit hijacked smart meters to launch ransomware attacks on energy management systems, or stealthily siphon energy from a municipality.

**Distributed denial of service (DDoS):** A denial-of-service attack (DoS attack) attempts to render a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting the services of a host connected to the internet. Within SC, a plethora of devices, such as parking meters, can be breached and forced to join a botnet that has been programmed to overwhelm a system by posting multiple simultaneous service requests.

**Permanent denial of service (PDoS):** A permanent denial-of-service attack (PDoS), also known loosely as phlashing, is an attack that damages the device so badly that it requires replacement or reinstallation of hardware. In an SC scenario, a hijacked parking meter could also fall victim to sabotage and would have to be replaced.

---

<sup>453</sup> <https://capec.mitre.org/data/definitions/94.html>

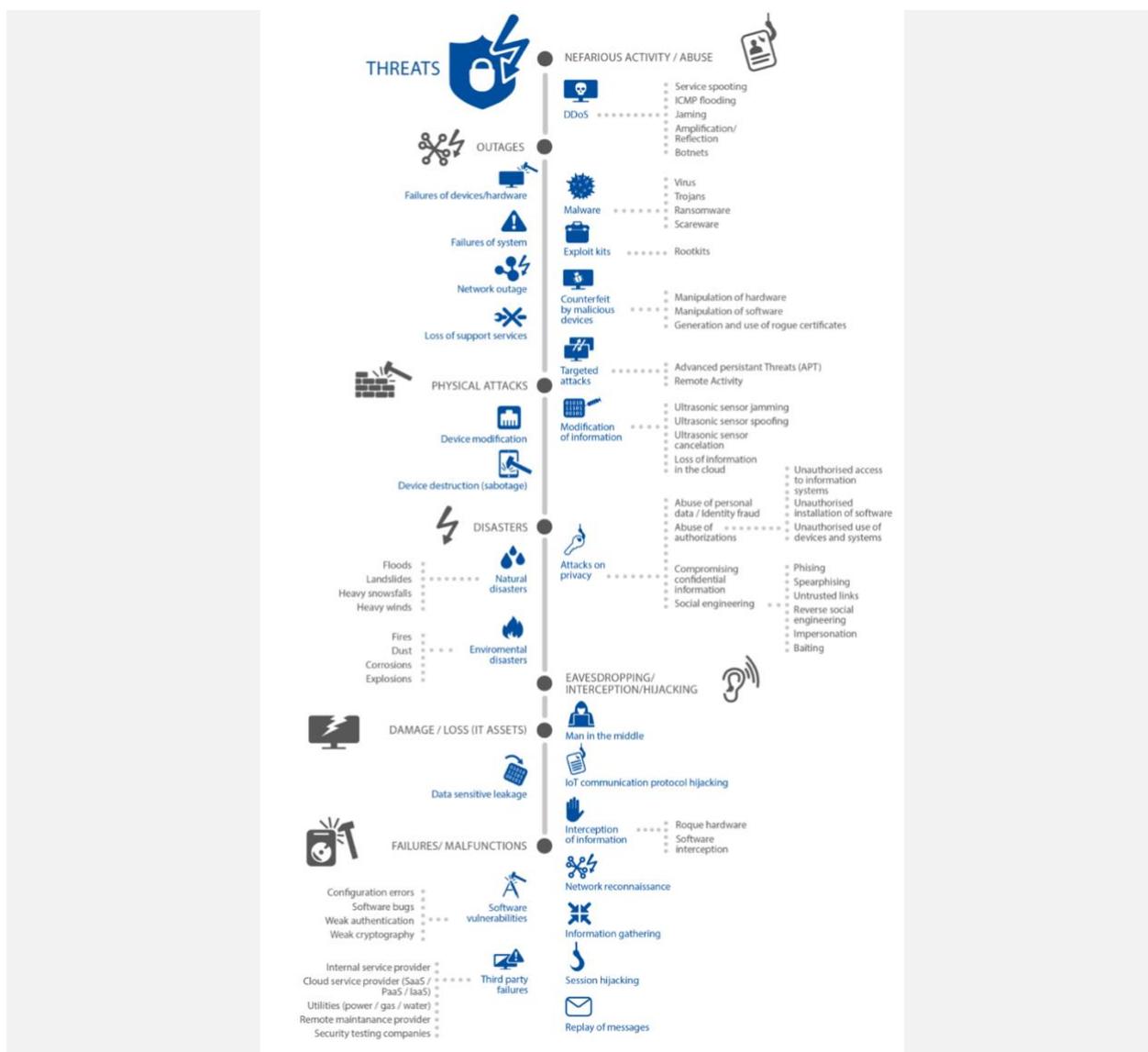


Figure 24: IoT Threat Taxonomy (Source: [ENISA 2018])

**Ransomware:** A type of malware that threatens to publish the victim’s data or constantly block access unless a ransom is paid. While some simple ransomware can block the system in a way that is not difficult for an experienced person to reverse, more advanced malware uses a technique called cryptoviral extortion, in which it encrypts the victim’s files, making them inaccessible, and requires a ransom payment to decrypt them.

From the human privacy standpoint, regulations have been slow to catch up with public concerns and to deal with the realities of privacy. Not being able to adapt new developments and technology-based solutions to a fast paced and changing environment is a threat in itself. Sustainability, health, safety and local economies are some of the concerns that need to be addressed, and if security is not fully accounted for, the very feasibility of those technologies might very well be threatened.

It is especially interesting and worth mentioning that security has stopped being a “selfish” matter, impacting only an individual domain or business, but has now become a global concern.

A good example is the *Mirai* botnet [KAMZ 2019], which took advantage of the lack of security of millions of IoT devices spread across the world to create a literal army of bots capable of bringing down entire systems, even countries, by generating the most powerful DDoS attacks ever recorded. In consequence, the security of your devices affects not only the users and owners of those devices, but also third parties around the world; this had never before been seen as a parameter in a risk-cost analysis for security. It is not unthinkable that, as happened with carbon emissions, governments and global agencies will impose regulations on the level of security required for connected devices to go public, on behalf of the public concern regarding global security.

### 9.3.3 What is the worst thing that can happen?

Following ENISA, different threats have different potential impacts [ENISA 2018]. Taking into consideration the threat taxonomy for IoT shown in Figure 24, and in Figure 25 provides a visual representation of the most dangerous threats and their impact, ranging from no importance to crucial importance.

Such threats may be used by attackers to cause cascade effects and further damage at different levels of the infrastructure. On this basis, the worst things that can happen if critical threats attack an SC **are likely to involve privacy and government crisis, SC lockdown, and also natural, industrial and safety disasters**. For instance, in the case of smart hospitals, an attack could lead even to people's deaths.

In an increasingly digital world, citizens need to be reassured that the local, regional and national government is able to protect its digital assets. Besides the physical impact, such as financial loss and lives at stake, the effect on citizens' trust in the capabilities of the cities to protect them and the utilities around them will be massive.

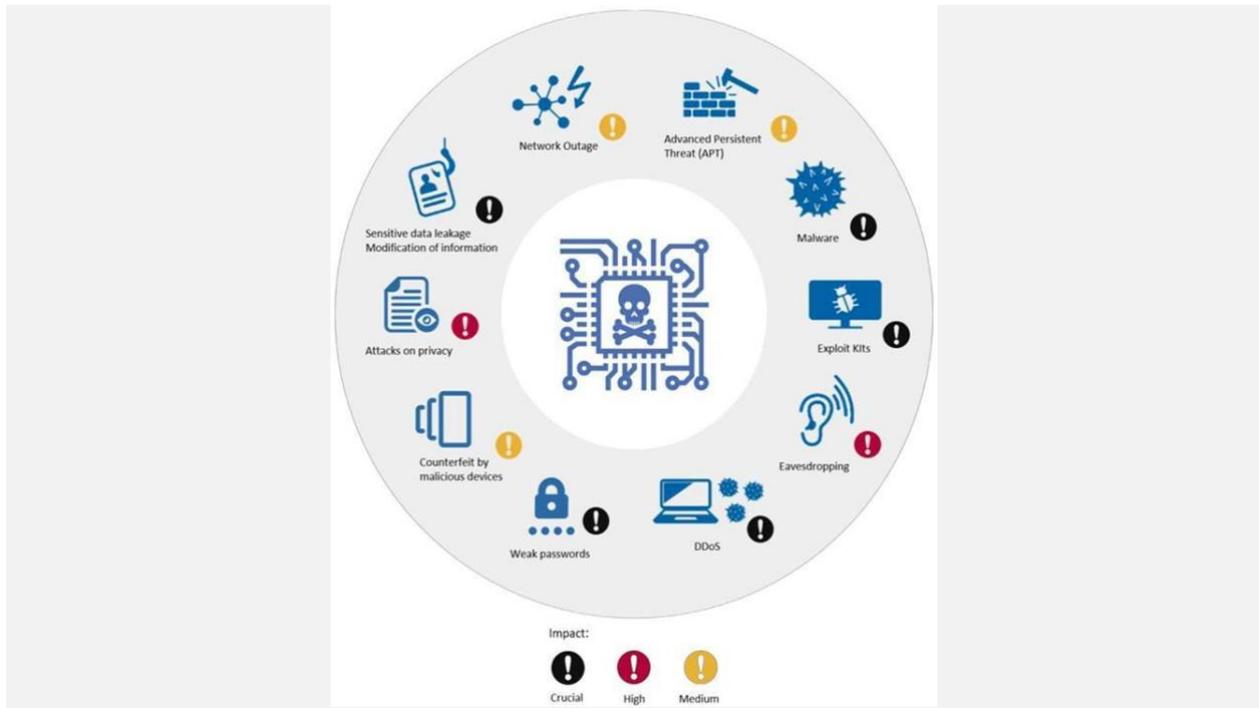


Figure 25: IoT Threats Impact

## 9.4 Who are the attackers?

In such a wide service scenario, Figure 26 lists the threat agents according to the **Intel Threat Agent Library** [INTEL 2007] (see Figure 26). The aim of this library is to provide a complete list of attackers (threat agents) and classify them by their intent, skills and common tactics. An important consideration to highlight is that such threat agents are not only motivated by financial intents, but may also be activists, spies, terrorists, vendors or, even unwittingly, employees.

Agent Label	Insider	Common Tactics/Actions	Description	
Anarchist		Violence, property destruction, physical business disruption	Someone who rejects all forms of structure, private or public, and acts with few constraints	
Civil Activist		Electronic or physical business disruption; theft of business data	Highly motivated but non-violent supporter of cause	
Competitor		Theft of IP or business data	Business adversary who competes for revenues or resources (acquisitions, etc.)	
Corrupt Government Official		Organizational or physical business disruption	Person who inappropriately uses his or her position within the government to acquire company resources	
Cyber Vandal		Network/computing disruption, web hijacking, malware	Derives thrills from intrusion or destruction of property, without strong agenda	
Data Miner		Theft of IP, PII, or business data	Professional data gatherer external to the company (includes cyber methods)	
Employee, Disgruntled	X	Abuse of privileges for sabotage, cyber or physical	Current or former employee with intent to harm the company	
Government Spy	X	Theft of IP or business data	State-sponsored spy as a trusted insider, supporting idealistic goals	
Hostile	Government Cyberwarrior	Organizational, infrastructural, and physical business disruption, through network/computing disruption, web hijacking, malware	State-sponsored attacker with significant resources to affect major disruption on national scale	
	Internal Spy	X	Theft of IP, PII, or business data	Professional data gatherer as a trusted insider, generally with a simple profit motive
Irrational Individual		Personal violence resulting in physical business disruption	Someone with illogical purpose and irrational behavior	
Legal Adversary		Organizational business disruption, access to IP or business data	Adversary in legal proceedings against the company, warranted or not	
Mobster		Theft of IP, PII, or business data; violence	Manager of organized crime organization with significant resources	
Radical Activist		Property destruction, physical business disruption	Highly motivated, potentially destructive supporter of cause	
Sensationalist		Public announcements for PR crises, theft of business data	Attention-grabber who may employ any method for notoriety, looking for "15 minutes of fame"	
Terrorist		Violence, property destruction, physical business disruption	Person who relies on the use of violence to support personal socio-political agenda	
Thief	X	Theft of hardware goods or IP, PII, or business data	Opportunistic individual with simple profit motive	
Vendor	X	Theft of IP or business data	Business partner who seeks inside information for financial advantage over competitors	
Non-Hostile	Employee, Reckless	X	Benign shortcuts and misuse of authorizations, "pushed wrong button"	Current employee who knowingly and deliberately circumvents safeguards for expediency, but intends no harm or serious consequences
	Employee, Untrained	X	Poor process, unforeseen mistakes, "pushed wrong button"	Current employee with harmless intent but unknowingly misuses system or safeguards
	Information Partner	X	Poor internal protection of company proprietary materials	Someone with whom the company has voluntarily shared sensitive data

Figure 26: Intel Threats Identification

## 9.5 Major incidents in this vertical

In terms of diffusion, one of the incidents with the most widespread impact was the **Mirai botnet** [KAMZ 2019], which took advantage of the lack of security of millions of IoT devices spread across the world to create a literal army of bots capable of bringing down entire systems, even countries, by generating the most powerful DDoS attacks ever recorded. In consequence, the security of your devices affects not only the users and owners of those devices, but also third parties around the world; this had never before been seen as a parameter in a risk-cost analysis for security. It is not unthinkable that, as happened with carbon emissions, governments and global agencies will impose regulations on the level of security required for connected devices to go public, on behalf of the public concern regarding global security.

Some other past attacks on SCs and their infrastructures, singled out from among the many, are described below:

- **Ukraine, December 23<sup>rd</sup>, 2015:** attackers compromised energy distribution, leaving 230,000 people without electricity [EISAC 2016].
- **Sweden, November 4<sup>th</sup>, 2016:** an attack affected several airports, preventing air traffic controllers from seeing aircraft on their screens. This resulted in the cancellation of multiple domestic and

international flights.<sup>454</sup> On October 11<sup>th</sup>, 2017, transport administration systems suffered a DDoS attack that resulted in disruption of services such as monitoring of traffic trains, agency email systems, websites and road traffic maps.<sup>455</sup>

- **San Francisco, November 25<sup>th</sup>, 2016:** municipal railway systems were infected by ransomware and the attackers demanded \$70,000.<sup>456</sup>
- **Sacramento, November 18<sup>th</sup>, 2017:** the regional transit system was attacked by ransomware [Bizjak 2019] that deleted 30 million files; the attackers demanded \$7000 in bitcoin.
- **Atlanta and Baltimore** have been subjected to massive cyber-attacks, experiencing different types of ransomware. Not only did the cities have to redeem the attack, paying hackers in return for keys to restore access to their systems, but cascading effects of the incidents also had a high-level economic impact, showing that a successful cyberattack can lead to a big disruption to business, a loss of reputation for companies and a loss of trust in emerging technologies from end users.
- In **March 2018, Atlanta** city was attacked by the *SamSam* ransomware, which was able to exploit multiple vulnerabilities. The Atlanta Journal-Constitution reported that it cost the city \$17 million to recover [Deere 2018]. More than a third of the 424 software programs used by the city were thrown off line or partially disabled in the incident. A month later, Atlanta reported that a malware attack (malicious software) had hit the police and legislative departments, wiping legal documents and dashboard camera evidence from their computers, at a cost that was assessed at \$12.2 million.<sup>457</sup>
- **Baltimore** is another example to take into consideration regarding high impact from cyberattacks. A first ransomware attack, thanks to highly vulnerable multiple entry points, was able to affect the city's computer-aided dispatch systems for emergency services (911 dispatcher), which were disrupted for 17 hours.<sup>458</sup> This system is used to divert calls to emergency responders who are closest to an incident and the task had to be performed manually by employees. IT experts and technicians at the department, isolated the affected server and fully restored the systems. In May 2019, another ransomware attack, a variant of the Robin Hood ransomware, held the city's computers hostage for 2 weeks. City employees were locked out of their email accounts and citizens were unable to access essential services, including websites where they pay their water bills, property taxes, and so on. This ransomware attack was the second in 15 months and cost the city about \$103,000.

## 9.6 Research Challenges

### 9.6.1 State of the Art

#### 9.6.1.1 Secure Data Sharing

The recent developments in the services offered by the project are based on the exchange of large amounts of heterogeneous data coming from different data sources, which are used to infer new knowledge and take more effective decisions. Therefore, from the security point of view, in order to achieve a sustainable

<sup>454</sup> [https://www.theregister.co.uk/2016/04/12/sweden\\_suspects\\_russian\\_hackers\\_hit\\_air\\_traffic\\_control/](https://www.theregister.co.uk/2016/04/12/sweden_suspects_russian_hackers_hit_air_traffic_control/)

<sup>455</sup> <https://www.scmagazineuk.com/ddos-attacks-delay-trains-halt-transportation-services-sweden/article/1473963>

<sup>456</sup> <https://www.forbes.com/sites/thomasbrewster/2016/11/28/san-francisco-muni-hacked-ransomware/>

<sup>457</sup> <https://www.reuters.com/article/us-usa-cyber-atlanta-budget/atlanta-officials-reveal-worsening-effects-of-cyber-attack-idUSKCN1J231M>

<sup>458</sup> <https://www.hackread.com/baltimore-911-cad-system-hacked-suspended/>

realization of SCs it is necessary to consider solutions aimed at enabling the protection of shared data, while still preserving the privacy of data owners. Towards this end, solutions based on Attribute-Based Encryption (ABE) approaches [SB 2005] have been widely proposed because of their high level of flexibility and expressiveness compared to traditional cryptographic solutions (i.e. symmetric and asymmetric cryptography).

In this direction, recent research works such as [PRG+ 2018, MEZ 2020, PJB+ 2020] consider the use of the Ciphertext-Policy ABE (CP-ABE) [BSW 2007] to protect confidential data. Specifically, [MEZ 2020] proposes the use of CP-ABE to encrypt the extension of the manufacturer's usage description and to implement limited access control policies and security aspects. Similarly, [PRG+ 2018] presents a lightweight and scalable encryption approach that combines the efficiency of symmetric key cryptography and the flexibility of the CP-ABE scheme to protect sensitive data in Smart Building scenarios, thereby avoiding unauthorized accesses. Additionally, in [PJB+ 2020] the authors implement a solution based on CP-ABE to secure the sharing of cyber threat intelligence (CTI) data between different organizations. They point out that CTI data sharing is a key aspect in the development of mechanisms that are able to detect, identify, determine and contain the incident and recover from cyber-attacks by collecting, analysing and sharing pieces of evidence. To this end, the use of threat intelligence platforms (TIPs) is considered, since they are cloud-based and on-premises distributed platforms that ease the aggregation and correlation of this type of information from multiple sources.

However, while CP-ABE approaches enable the protection of confidential data and make it accessible only by the group of authorized entities, there is also another type of information whose disclosure could harm the privacy of data owners and therefore needs to be obfuscated. Towards this end, the application of privacy-enhanced technologies (PETs), such as anonymity, perturbation or differential privacy, could be employed as mechanisms to achieve the obfuscation of such information, thereby preserving privacy. In this context, the literature provides different proposals that envisage PET techniques to protect the privacy of stakeholders during the data sharing process. In particular, in [BO 2020] the authors propose a pseudonym strategy to achieve location privacy in vehicular networks. The singularity is that the vehicle changes its pseudonym when it reaches a roadside unit, instead of changing it when a certain number of vehicles are found in a specific place. Similarly, [AAK+ 2018] presents an algorithm based on minimum instance disclosure risk generalization that aggregates random samplings in groups to preserve the privacy information. It is based on the Angel [TXZ+ 2020] technique, which refers to basic principles such as k-anonymity, l-diversity or t-closeness and adds correlation preservation while preserving privacy. According to the results and advantages pointed out in the previous research works, the CP-ABE scheme emerges as a potential security solution that may be considered to properly protect shared confidential data (e.g. CTI data) in the SC context, while the privacy of involved entities is still preserved by the use of PET techniques.

Currently, many businesses are struggling with the definition of appropriate procedures and technical solutions for their development process so as to enforce and demonstrate GDPR compliance [CDM 2019; FS 2018; ASS+ 2018; BMF+ 2018]. More precisely, they recognized as a key factor the availability of automated support for specifying privacy requirements, controlling personal data and processing them in compliance with the GDPR.

From a practical point of view, scientific communities and private companies are identifying in the consent and security services the successful elements for automatic specification and enforcing the data protection

regulation [RS 2017; RSS+ 2017; BDH 2018; M-APP 2020]. Indeed, the consent services may allow citizens and companies to manage and track personal data in an easy and user-friendly manner, while the security services, and specifically the authorization systems (Access Control [AC]), can enforce the data protection regulations, taking into account additional legal requirements such as the purpose of the data use, user consent and the data retention period.

Therefore, the joint work of the consent and security services may overcome the difficult and error-prone task of extracting legal machine-readable policies directly from the GDPR's rules. Currently, different research activities have been devoted to define and implement privacy knowledge and rules [PPM 2011; BCM 2019, BDL+ 2019], but no generic solution is yet available. Along these lines, under the hypothesis that the joint integration of access control systems and consent managers can enhance the controller's and processor's compliance with the regulation, Bartolini et al. [BDL+ 2019] are aiming to provide the basic architecture of a generic and practical solution to solve the GDPR compliance problem.

In this context, blockchain and distributed ledger technologies (DLTs), or their combination with other technologies, could support SCs and governments to reduce fraud and errors, and by design can provide transparency over data transactions. Governments worldwide are experimenting with blockchain to better meet the needs of public-service users and organize the coherent use of resources to maximize public value. Blockchain and DLT technologies are not yet fully established in public services, and it is therefore necessary to experiment with their integration into the public innovation ecosystem. The European Council has promoted a European approach to blockchain in order to harness its many opportunities and support actions at government level to avoid a fragmented approach.<sup>459</sup> The Declaration of Cooperation on a European Blockchain Partnership recognizes the potential of blockchain to transform digital services in Europe:

- to change the way citizens and organizations collaborate, share information, execute transactions, organize and deliver services.
- to enable more decentralized, trusted, user-centric digital services, and stimulate new business models benefiting our society and the economy.

The close cooperation between Member States towards a European ecosystem for blockchain services will reinforce the chances of developing the right conditions for this technology. The European Blockchain Partnership (EBP) is working on establishing a European Blockchain Services Infrastructure (EBSI) that will support, in a first stage, the delivery of cross-border digital public services, while meeting the highest standards of security, privacy, sustainability and compliance with EU laws. One of the 4 initial use cases defined by the EBP Policy Group is focused on "*Identity*", aiming at a European Self-Sovereign Identity (SSI) Framework that allows citizens to create and control their digital identity and securely authenticate with businesses and governments.

Recently, the acceptance of and interest in DLT and blockchain technologies, not only in the scientific field, but also in the more ordinary context, has surged. Thus, various research has been geared to this topic. Different approaches are similar to the ideas used in this vertical in certain respects, such as, for example:

---

<sup>459</sup> <https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy>

[VAO 2021] which deals with the implementation of an access control framework for SC with the support of blockchain, and [CSKP 2021], which is centred on a cloud architecture based on secret sharing for SC.

Given the complexity of SC infrastructures, the traditional monitoring approaches (based on attack signatures and anomaly detection) could be ineffective. This calls for different approaches, such as those based on artificial intelligence and machine learning [LP 2018] to learn hidden patterns, and those aiming to verify the infrastructure integrity in order to detect software and hardware manipulations [DBL 2019]. These concepts are behind two research lines in this work package, namely machine learning to detect attacks hidden inside encrypted network channels, and attestation of the integrity state of a network infrastructure, based on trusted computing technologies

### 9.6.1.2 Cyber Risk Assessment

AgID, “Agenzia per l’Italia Digitale” is the Italian agency that has to provide guidelines for Italian public administrations (PAs) in their path of digitalization. It is the main point of reference for Italian PAs, Genoa included. With regard to risk assessment, the Italian agency suggests that PAs should “identify an IT risk management methodology”, starting from the “definition and analysis of the context (internal and external) of the PA, so as to identify the peculiarities that characterize this context and the possible set of threats to which it may be exposed.”

What has failed in the risk assessment conducted into the PAs so far is the assumption that they could be modelled as an organization like companies. This is not feasible, because this view does not take into account the *peculiarities of the context* and the real *objectives* of a PA (obviously different from those of a company).

Depending on the complexity of the information system and the organizational reality of the administration, risk management activities can translate into technological, organizational and procedural controls useful for assessing the level of IT security and aimed at combating the most frequent cyber threats, within a continuous process of monitoring and improvement.

AgID also refers to ISO, NIST and ENISA guidelines and standards in order to determine the state of the art in this field. In the self-assessment phase, the one the project is demonstrating in WP5, the assessment that AgID suggests for PA services consists of accurate mapping of the services in order to ensure a timely and reliable calculation of the level of risk. The methodological approach chosen by AgID is based on the principles and guidelines dictated by the ISO 31000 standard and on the information risk assessment methodology 2, a methodology produced by the Information Security Forum (ISF). The methodology makes it possible to assess the risk associated with a certain threat with respect to the services provided or used by a PA, without affecting the assets that compose them.

In the common approaches used for risk assessment so far, experts’ opinions were always an indispensable step in the risk evaluation; however, in a smart city context, active human participation cannot be provided for the huge, complex, and permanently changing digital environment of the smart city. A recent study

[KKV 2021] has explored a new methodology for assessing cyber risks in a smart city environment, using an artificial neural network. The approach is based on object typing, data mining and quantitative risk assessment. Thanks to the neural network, it shows how to automatically, unambiguously and reasonably assess the cyber risk for various object types in the dynamic digital infrastructures of the smart city.

Regarding the available frameworks in this field, from CyBOK [CyBOK2019] it is possible to extract the most recent list of commonly used component-driven cyber risk management frameworks.

- ISO/IEC 27005:2018<sup>460</sup> is an international standard set of guidelines for information risk management. It does not prescribe a specific risk assessment technique but does have a component-driven focus and requires vulnerabilities, threats and impact to be specified.
- NIST SP800-30/39<sup>461</sup> are the US Government's preferred risk assessment/management methods and are mandated for US government agencies. They have a strong regulatory focus, which may not be relevant for countries other than the US, but they have a clear set of guiding steps to support the whole risk assessment and management process from establishing context to risk tolerance, and effective controls, including determining likelihood of impact.
- The Information Security Forum (ISF) produced the IRAM 2 risk management methodology,<sup>462</sup> which uses a number of phases to identify, evaluate and treat risks based on vulnerability, threats and impact measures. It is provided to (paid up) members of the ISF and requires information risk management expertise to use it effectively, which may come at additional cost.
- FAIR, initially developed by Jones and subsequently collaboratively developed with the Open Group into OpenFAIR,<sup>463</sup> proposes a taxonomy of risk factors and a framework for combining them. The threat surface can be considered very broad, and there is a clear focus on loss event frequency, threat capability, control strength and loss magnitude. It also breaks financial loss factors into multiple levels and supports a scenario model to build comparable loss profiles.
- Octave (Operationally Critical Threat, Asset, and Vulnerability Evaluation<sup>SM</sup>) Allegro<sup>464</sup> is oriented towards operational risk and security practices rather than technology. Qualitative risk assessment is linked with organisational goals. Real-world scenarios are used to identify risks through threat and impact analysis.
- STRIDE<sup>465</sup> is a failure-oriented threat modelling approach focusing on six core areas: spoofing (faking identity), tampering (unauthorised modification), repudiation (denying actions), denial of service (slowing down or disabling a system), and elevation of privilege (having unauthorised control of the system).

Attack Trees<sup>466</sup> formulate an overall goal based on the objectives of an attacker (the root node), and develop sub-nodes relating to actions that would lead to the successful compromise of components within a system. Like STRIDE, attack trees are required to be iterative, continually considering pruning the tree and checking

---

<sup>460</sup> <https://www.iso.org/standard/75281.html>

<sup>461</sup> <https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final>

<sup>462</sup> <https://www.securityforum.org/solutions-and-insights/information-risk-assessment-methodology-iram2/>

<sup>463</sup> <https://www.fairinstitute.org/blog/what-is-open-fair-and-who-is-the-open-group>

<sup>464</sup> <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419>

<sup>465</sup> [https://en.wikipedia.org/wiki/STRIDE\\_\(security\)](https://en.wikipedia.org/wiki/STRIDE_(security))

<sup>466</sup> [https://en.wikipedia.org/wiki/Attack\\_tree](https://en.wikipedia.org/wiki/Attack_tree)

for completeness. Attack libraries such as Common Vulnerabilities and Exposures (CVEs) and Open Web Application Security Project (OWASP) can be used to augment internal knowledge of evolving threats and attacks

### 9.6.1.3 Social Engineering and Phishing

There are many different definitions of Social Engineering (SE), but the following is interesting because it is classic and belongs to the so-called “old-school” SE and at the same time it is also generic enough to contain hints on what is nowadays SE 2.0: “Social Engineering (SE), in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional “con” in that it is often one of many steps in a more complex fraud scheme. The term “social engineering” as an act of psychological manipulation is also associated with the social sciences, but its usage has caught on among computer and information security professionals”.<sup>467</sup>

A basic bibliography of the old SE school includes (e.g. the ability of D. Mitnick or Frank William Abagnale Jr. to trick humans)<sup>468</sup> [Granger 2001][MSW 2006][MS 2009]. At its roots, the early social engineers were all IT experts or talented hackers. Despite being well prepared in hacking logics and personally talented, their results were not comparable to the results achievable nowadays through the involvement of professionals such as psychologists, marketing experts or cognitive scientists in the hacking attacks. The modern SE includes and extends these concepts.

The main problem is that the number of automatic attacks exploitable against a large number of people at the same time has increased greatly in recent years. Almost all the mainstream security companies are focusing on how the human mind could be hacked and most of all how it can be protected.

SE is a well-known method of deception, used since historic times. What has completely changed the landscape in recent years, are the following two important evolutions:

- The evolution of the social network through mobile platforms and corresponding new habits.
- The appearance of some new technologies that allow a high level of automation of most of the SE steps against a large number of people/victims at the same time.

These two factors contributed to the evolution of SE into a new and multifaceted phenomenon called Social Engineering 2.0, [SE 2.0], which has increased the number of potential victims directly exposed on the internet. It uses advanced automatic methods to gather and elaborate the information needed to carefully select the “victims”.

SE 2.0 is indeed a complex phenomenon that involves several heterogeneous technologies and competences, such as modern OSINT (Open Source Intelligence): modern SE techniques use data mining techniques to

---

<sup>467</sup> [https://en.wikipedia.org/wiki/Social\\_engineering\\_\(security\)](https://en.wikipedia.org/wiki/Social_engineering_(security))

<sup>468</sup> <http://phrack.org/issues/67/15.html>

derive information from data. The amount of data available on the net is huge. Information abused for bad purposes is a huge opportunity to improve the efficiency of information gathering in an SE attack.

In the 2020, ENISA published the “ENISA Threat Landscape” about phishing, which includes numbers showing the scale of the problem nowadays:

- 26.2€ billions of losses in 2019 with Business E-mail Compromise (BEC) attacks
- 667% increase in phishing scams in only 1 month during the COVID-19 pandemic
- 32.5% of all the e-mails used the keyword “payment” in the e-mail subject

According to some recent projections,<sup>469,470,471</sup> phishing attacks targeting software-as-a-service (SaaS) and webmail services surpassed those against payment services for the first time in Q1 2019, making them the most targeted sector, at 36% of all phishing attacks. This new record follows the trend in 2018, when SaaS and webmail services had just overtaken the financial sector.

Today, companies are increasingly carrying out simulated phishing campaigns to test the vulnerability of their human layer of security. In other words, testing how easily their employees fall for SE-based attacks delivered by emails (mainly phishing ones). This market was almost nonexistent until a few years ago, while today a growing number of companies offer simulated phishing frameworks. It is also in rapid growth, as demonstrated by several big acquisitions and significant capital investments.

Players like Wombat and Knowbe4 are deliberately concentrating on the risk detection functionalities and mainly use the Social Driven Vulnerability Assessment (SDVA) as a way to (a) convince customers to buy the related awareness and training programs, (b) to demonstrate the effectiveness of the awareness and training programs sold, and (c) concentrate almost entirely on simulated phishing SE-enabled attacks. This is also proved by the fact that they appear in Gartner’s magic quadrant of “Security Awareness Computer-Based Training”.<sup>472</sup> In this sense, they even are more advanced than other players in the same market (e.g. Inspired eLearning, Cofense, JungleMap and others) that adopt a much more simplistic approach delivering training without running any periodic assessment to measure how the training and awareness program contributed to mitigating the risk of being compromised.

While GDPR compliance is relatively simply to achieve from a technical point of view (as some market leaders such as KnowBe4 and Proofpoint have already done), a more comprehensive SELP compliance requires much more work and is considered as a key factor supporting effective EU market penetration. In fact, there is a trade-off between, on the one hand, the respect of SELP principles and regulations and, on the other, the need to conduct assessments as close as possible to real SE-based attacks, which does not follow any ethical or legal rule. If the operator carrying out the simulated SE attack does not have a clear picture of the legal and ethical implications of the attack, especially if the simulation product does not

---

<sup>469</sup> <https://www.vadesecure.com/en/phishers-favorites-q2-2019/>

<sup>470</sup> [https://info.phishlabs.com/hubfs/2018%20PTI%20Report/PhishLabs%20Trend%20Report\\_2018-digital.pdf](https://info.phishlabs.com/hubfs/2018%20PTI%20Report/PhishLabs%20Trend%20Report_2018-digital.pdf)

<sup>471</sup> [https://docs.apwg.org/reports/apwg\\_trends\\_report\\_q1\\_2019.pdf](https://docs.apwg.org/reports/apwg_trends_report_q1_2019.pdf)

<sup>472</sup> <https://www.gartner.com/en/documents/3950454/magic-quadrant-for-security-awareness-computer-based-tra>

provide the proper assistance, his/her attempts to be on the safe side of the legal compliance will result in weak and predictable SE attacks. Compliance is also important when running controls on the sites that employees are trying to visit, or when assessing the results of a training campaign.

According to Verizon DBIR report,<sup>473</sup> the average time taken to click a phishing email is 82 seconds. Consequently, incident response systems need to be able to automatically detect and respond to SE attacks in real time. Despite the basic and “easy-to-implement” measures to mitigate such risks, such as SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) and DMARC (Domain-based Message Authentication, Reporting, and Conformance), these are not enough to mitigate the majority of SE attacks. Nowadays, numerous tools protect organizations against phishing attacks: these include RSA FraudAction,<sup>474</sup> which detects and mitigate phishing sites; Avanan,<sup>475</sup> which enhances the security of Office 365; Barracuda Sentinel,<sup>476</sup> which monitors inbound email and identifies accounts that may have become compromised, remediating these accounts by detecting and deleting malicious emails sent to other internal users, notifying external recipients, locking the account, and even investigating inbox rules that may have been created by the malicious user; and IRONSCALES<sup>477</sup> for email security, which combines AI-based identification and human interaction (through notifications) to quickly respond to potential attacks while simultaneously limiting false positives

## 9.6.2 SWOT Analysis

Figure 27 provides a summary of the SWOT which is analysed in the sections below.

---

<sup>473</sup> <https://www.verizon.com/business/resources/reports/dbir/>

<sup>474</sup> <https://www.rsa.com/en-us/products/fraud-prevention/phishing-protection>

<sup>475</sup> <https://www.avanan.com/anti-phishing-software>

<sup>476</sup> <https://www.barracuda.com/products/sentinel>

<sup>477</sup> <https://ironscales.com/>



Figure 27: Smart Cities SWOT Summary

### 9.6.2.1 Strengths

- The EU is paying increasing attention to technological solutions** that are able to improve the management and efficiency of the SC environment. Indeed, research proposals and tools specifically conceived for SC systems and their environment are, on the one hand, important means for assuring mitigation and avoidance of the cybersecurity and privacy risks at all IoT levels. On the other hand, these research proposals and tools are fundamental for improving citizens' quality of life and increasing the competitiveness of European cities and industries. Specifically, the improved technologies, services and communication will:

  - enable SCs and their administration to make better use of the available resources and data;
  - encourage active competition between cities to attract capital, residents, and tourists;
  - improve the quality of life;
  - increase the quality of provided services;
  - improve the efficiency and effectiveness of communication with citizens;
  - Reduce the financial burden and the consumption of resources.
- Increasing the connectivity and interactions between humans, the environment and smart devices will increase the opportunities for EU companies and project partners to develop more**

**effective, human-centric and smarter solutions** for cybersecurity and privacy failure prevention, thanks to the larger amount of data to analyse and model. The innovative technologies and the simpler communications will enable EU SC to make better use of their resources, save money, and increase trust in the services provided.

- The newly conceived SC business processes, together with the information and communication protocols, will contribute to the adoption of governance guidelines that can reduce crimes, increase the level of situational awareness, provide effective and efficient response to accidents and emergencies, and improve the SC municipal services. From a technological point of view, this will promote:
  - the development of common taxonomies, ontologies and data sets useful for promptly identifying cyber-physical vulnerabilities and threats (such as privacy, data & identity theft, device hijacking, denial of service, and man-in-the-middle attacks and ransomware).
  - the by-design development of shareable, open source, effective and efficient solutions for avoidance, protection, verification and validation processes
- Introducing diversity in management and technologies, rethinking and reframing of the current architectures and approaches, will **increase the opportunities for EU companies and project partners to conceive solutions focused on** efficiency, efficacy and quality. Because of their complexity, SC are one of the most appropriate environments for the benchmarking adoption of innovative technologies such as AI, Digital Twins, and machine learning. They are also a very generic ecosystem able to challenge and promote the development of efficacious means and methodologies for assessing the impact of SC tools, solutions and proposals on the community before their commencement. As a side effect, the SC innovations will leverage the function, interoperability, and compatibility between different SCs, but will also improve and assess global understanding of their impact on the community and the overall SC ecosystem.

**Data Security and Protection:** The continuous evolution and improvement of the SC ecosystems constantly provides new challenges and forces ongoing refinement and rescheduling of the general EU recommendations and guidelines for Cyber data protection and security. This will increase accountability and, in turn, gives EU citizens the assurance of responsible management of their private data. In parallel, interconnected ecosystem of secured and trusted platforms, where EU SC citizens are carefully authenticated, authorized and managed, will increase the overall EU level of technology adoption.

### 9.6.2.2 Weaknesses

- Despite the increasing interest in the research and industrial environment for SC applications and developments, **there are still intra- and inter-portability and integration issues to be solved.** There are still hw/sw differences between the different SCs, resulting in fragmentation that makes it difficult to adopt the same technology in different environments. Common platforms of unified services are still necessary to integrate heterogeneous implementations of various countries and cities.
- There is still a need for integrated, online, holistic Verification and Validation (V&V) solutions for the evaluation and assessment of SC components and services in the SC infrastructure. Additionally, the impact of the infrastructures and applications on different environments and ecosystems, as well as on the community and individuals, needs to be properly evaluated. The V&V activities should

focus not only on designs and architecture functions, interoperability and compatibility, but also on the impact on people and communities, as well the satisfaction of their privacy and security needs.

### 9.6.2.3 Opportunities

- The COVID-19 pandemic has greatly emphasized the need to relocate workstations, moving them from the office to employee homes or public parks. This has introduced huge security and privacy issues that must also be addressed from a smart city infrastructure perspective, opening an important market.
- EU companies can exploit the possibility of developing solutions and components that provide effective protection and are sufficiently flexible to be easily adopted in different environments. This will provide new opportunities within a significant segment of the market. Indeed, proposals that can improve the control and validation of security, privacy as well as methods for monitoring the quality, trust and compliance of the different SC components are definitely required.
- Improvement in SC development. This will improve the EU's adoption of technologies and means for hazards (such as fires, leaks, etc.), monitoring, prevention, visualization and decision-making approaches and techniques. Finally, the management of enormous amounts of data will increase EU research into the optimization of resources, improvement of the effectiveness of SC resources, and reduction of the resources required.

### 9.6.2.4 Threats

- Threats due to the continuous evolution of cyber and physical attacks: EU companies are focusing their attention on specific city services, without a global vision of cybersecurity. Without considering the cybersecurity issues that derive from the interoperability among multiple infrastructures in the same network, vulnerability and threats are still possible. Additionally, their continuous change and evolution could make security technologies obsolete too soon, thwarting efforts towards technological progress and making the threats impossible to prevent.
- Threats due to the lack of global adoption of the common security and privacy regulations: EU companies may be reluctant to adopt the enforcement of global security regulations, such as the GDPR or others focused on access to resources and data, opening the path to security and privacy issues. In SCs, the availability of enormous amounts of data, generated in real time by different groups of users and by multiple heterogeneous data sources, may lead to difficulty in their management and understanding

### 9.6.3 European Digital Sovereignty

With the new strategy “Europe fit for the digital age” and large sources of funding – particularly linked to the COVID-19 pandemic and support for recovery (see 3.5.5) – the EU aims to ensure Europe’s technological sovereignty. The focus of the German EU presidency on strengthening Europe’s digital and technological sovereignty stresses the importance of this topic: “Secure and sovereign, European-based, resilient and sustainable digital infrastructure is essential to this transformation. Creating this singularly European digital economic realm is key to keeping the EU competitive in a technological sphere dominated by the United States and China”.<sup>478</sup>

Another suggestion comes from the BDVA position paper. A technical challenge regarding the digital sovereignty is to reinforce data usage rights: “The realisation of a mixed data sharing space will only materialise if data producers are guaranteed to retain their rights as the original owners ... enabling them to retain control of who can use their data, for what purpose and under which terms and conditions. To guarantee digital sovereignty, different ownership models or suitable data rights management frameworks need to be further explored” [BDVA 2020]. Here the SC vertical provides the municipality with CaPe: a tool for consent management that strengthens citizens’ rights with regard to controlling their data.

In SC environment, digital data sovereignty is feasible and effective at EU level, through the General Data Protection Regulation. It might be reasonable to move in the same direction when it comes to AI sovereignty and 5G sovereignty, to name two key digital areas potentially disruptive for SCs. Because the best response to multinational giants’ digital control (Google, Apple, etc.) is the establishment of supranational digital sovereignty (de jure and not only de facto), at EU level.

Contributions:

- Open building blocks for secure and trusted data sharing for cities and regions
- Upskilling work force
- Interoperability

### 9.6.4 European Digital Sovereignty

### 9.6.5 COVID-19 and Public Health Dimension

In the COVID-19 era the SC ecosystem has also been affected and forced to react promptly to new challenges, such as:

- Switching from standard face-to-face data collection methods to remote data collection, i.e. collection of data via the phone, on line, or other virtual platforms, with the person involved physically distant. These consultations oblige SC to pay more accurate and lawful attention to sampling and recruitment, informed consent, response rates, rapport with participants, privacy and safety, and data analysis.

---

<sup>478</sup> <https://www.eu2020.de/eu2020-en/eu-digitalisation-technology-sovereignty/2352828>

- Using data-driven smart applications that efficiently manage sparse resources and city operations in efficient and secure ways.
- Developing SC systems and architectures capable of providing fast and effective mechanisms to limit the further spread of the virus. These include the implementation of active surveillance, monitoring and enforcing social distancing between people.
- Dealing with secure, safety- and privacy-preserving management of real-time data. This leads to better informed and improved decision making inside the SC. Consequently, the pandemic is fuelling a digital transformation of public authorities. They need to use smart technologies to assess cyber threats and ensure secure sharing of personal and non-personal data.

Living at a social safety distance. The digital transformation of cities and regions open the path a set of smart activities (such as teleworking, e-government, communication and digital democracy) that have definitively changed our daily life. Consequently, in order to maintain democracy and equality, supporting human centric technologies and application should be developed and made available at all social levels.

Within this project, different assets have contributed (or are still contributing) to facing the SC challenges posed by COVID-19. ENG has already a product on the market called Eng-DE4Bios,<sup>479</sup> a bio-surveillance platform that enables monitoring of the evolution of the epidemic, mapping and geolocation of infected subjects, and identification of clusters requiring higher attention. Based on the Digital Enabler, the ecosystem platform allows the integration, harmonization, correlation and visualization of scattered and multi-source data, taking care of secure and trusted sharing of personal data (health data, infection rates, crowd sizes, etc.). Eng-DE4Bios has been used in Regione Veneto with great results.<sup>480</sup>

The impact on the public health dimension was recently demonstrated to citizens by the “Impacts of AI and Blockchain on Smart Cities” panel, during the Strategy Innovation Forum (SIF) 2021 of University Ca’ Foscari in Venice. The use of this new technology made it possible to lower the contagiousness index from 3.4 to 0.7 in two months. That proved to be a decisive tool for the regional task force in charge of containing the epidemic. Other future advice from the forum is the creation of a common European health data space, in order to allow the world’s health authorities to use data as an essential resource to more promptly cope with the spread of the virus.

CNR is exploring the possibility of adopting indoor localization technologies to measure distances between users in interior spaces. Moreover, a reference architecture for an Indoor Localization System (ILS), has been proposed, and its use within three representative use-cases has been illustrated. Specific attention has been devoted to the exploration of the privacy and trust reputation of an ILS during the discovery phase, and the deployment of the ILS in real-world settings

### 9.6.6 Green Deal and Climate Change

Human activities are the undeniable main factor in Earth’s climate changes. An increase in the world’s temperature, progressive desertification, and various other long-term alterations of weather patterns are directly or indirectly caused by human beings. About 55% of the world’s population lives in urban areas,

---

<sup>479</sup> <https://www.eng.it/en/our-platforms-solutions/eng-de4bios>

<sup>480</sup> <https://www.internationaldataspace.org/a-biosurveillance-system-for-the-protection-of-citizens-against-covid-19/>

and this percentage is expected to rise to 68% by 2050.<sup>481</sup> Cities therefore bear the major responsibility for the world's production of pollution, and climate change in general. In this context, the adoption of new, smarter, and safer technologies will, hopefully, reduce or reverse the damage to our planet's weather. However, the SC of the future will also have to face many challenges to make this happen.

Energy consumption is one of the most impactful causes of pollution. The adoption and development of green computing tactics will leverage both hardware and software techniques to achieve eco-sustainable IT systems and green cloud environments. Although many of these concepts are not new, there are some recent ideas regarding their large-scale adoption in SC environments [BCS 2021]. Using fewer resources and less power-hungry devices, however, will be particularly challenging since the rise of cryptographically secure protocols (e.g. HTTPS) and machine-learning techniques (used in IDSes and other monitoring controls), which are notoriously greedy for computational power. Another big factor in pollution and climate change is the emission of greenhouse gases (e.g. CO<sub>2</sub>). Autonomous vehicles are still in their infancy, but they promise to revolutionize urban transport systems. Their self-driving capability will allow them to take smarter routes to a destination, potentially allowing a drastic reduction of the traffic in a city. Their potential large-scale adoption in the future, however, will require many challenges to be overcome, such as making them as invulnerable to cyber-attacks as possible. In addition, since the COVID pandemic struck our planet, it is reasonable to assume that the number of employees adopting smart working will increase, thus further reducing their need to use private or public transportation. The adoption of electric scooters and other vehicles has already started in several major cities, and this trend will help improve citizens' mobility, at the same time reducing pollution at the cost of requiring more electrical energy. Striking the right balance between consuming less power and generating less greenhouse gases will be critical in the near future.

Forest fires, river floods, and climate disasters are calamities that can be either triggered by natural causes or not (e.g. as a direct consequence of pollution). In either case, every city must find a reliable way to cope with them and to prevent them, if possible. The adoption of satellite imaging, 5G technologies, IoT devices and wireless sensor networks has already started helping modern SC to perform early detection of perilous situations.<sup>482</sup> Deploying a vast array of sensors scattered through the urban area will provide smart cities with an early warning system that is able to detect imminent disasters. Even if some disaster prevention systems have proved to be fallible, most notably the anti-flooding system installed in the Chinese city of Zhengzhou,<sup>483</sup> it is reasonable to assume that the adoption of sensor networks and satellite imaging will play a big role in safeguarding the SC of the future. From a cybersecurity point of view, the biggest challenge will be to protect these arrays of IoT and 5G devices. On the positive side, there is already a good amount of literature investigating the security issues and protection techniques for weak IoT devices, even in SC scenarios [ZLA+ 2021, ZLL+ 2021].

According to the Food and Agriculture Organization, food security is defined as: when all people, at all times, have physical, social and economic access to sufficient, safe and nutritious food that meets their

---

<sup>481</sup> <https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html>

<sup>482</sup> <https://spectrum.ieee.org/how-iot-makes-fire-detection-systems-smarter>

<sup>483</sup> <https://www.scmp.com/tech/big-tech/article/3142898/china-floods-smart-city-system-capabilities-called-question-after>

dietary needs and food preferences for an active and healthy life. On one hand, cities require a great amount of drinkable water and food. On the other hand, they produce a great amount of food and water waste and this will tend to increase over time. At the same time, land for agriculture and herding is starting to become scarce, also because of the apparently unstoppable desertification of several regions. The scientific literature has recently started to provide some ideas for better managing cultivated lands to produce more food with less waste and resources. Some research hints at the use of AI methodologies to optimize agricultural food production [SKS+ 2021], while others propose the adoption of IoT devices for constantly monitoring the food production processes [WMK 2021]. Since the ever-growing adoption of self-driving drones, machines and IoT devices will continue in the foreseeable future, protecting the food supply chains from cyber-threats will become more and more paramount, since a surgically placed cyber-attack on these highly automatized environments will be able to cripple an entire city's food supply.

### 9.6.7 Impact on Democracy

The ubiquitous diffusion of sensors, IoT appliances, sensor networks, actuators and a variety of smart devices is a key concept for the SC paradigm. The proliferation of such startling numbers of interconnected devices that quietly monitor and intelligently react to the surrounding world has already started to have a deep impact on human interactions in several cities around the world.

Smart cameras and sensors in general can be used for a variety of life-improving and life-saving purposes. However, their rightful use is still a grey area. These networks of surveillance devices can be used to monitor citizens and potentially perform unwanted surveillance of people. For instance, in 2020, the San Diego Police Department used a number of cameras embedded in smart streetlights to keep track of several protestors in the roads, plazas and public places.<sup>484</sup> A utopic self-adapting SC sounds like a dream come true. However, the rightful use of its monitor devices will need to be properly regulated by laws to guarantee its citizens their freedom in public areas. In 2019, Shanghai started the deployment of City Brain, a continuous monitoring system that gathers the data from thousands of facial recognition cameras scattered through the city for identifying crowds, people dumping garbage and so on, in real time.<sup>485</sup> One of the biggest challenges is thus constant surveillance, which may risk transforming the smart cities of future into “surveillance states” like that in George Orwell's novel, “1984”.

Achieving perfect computer and network security is a chimera. Every hardware and software system is vulnerable and subject to attacks that can lead to more or less serious repercussions. Living in an SC filled with technologies will certainly help the quality of our lives, but potentially will also increase the cyber-attacker's surface area. Increasing the complexity of a system and its component also increases its vulnerabilities. In a such an interconnected world, where everybody has access to everything, the potential for cybercriminal and hacktivism activities is high and will most likely continue to grow in the foreseeable future. According to the Berkeley survey “The Cybersecurity Risks of Smart City Technologies”,<sup>486</sup> several experts ranked the emergency and security alert systems as the most vulnerable to cyber-attacks, followed by street video surveillance and smart traffic lights. In addition, the interviewed experts also concluded that nation-states and insiders would be most effective at executing cyber-attacks, closely followed by

---

<sup>484</sup> <https://gcn.com/articles/2021/08/13/smart-city-dystopia.aspx>

<sup>485</sup> <https://asia.nikkei.com/Business/China-tech/Shanghai-district-installs-comprehensive-surveillance-system>

<sup>486</sup> [https://cltc.berkeley.edu/wp-content/uploads/2021/03/Smart\\_City\\_Cybersecurity.pdf](https://cltc.berkeley.edu/wp-content/uploads/2021/03/Smart_City_Cybersecurity.pdf)

cybercriminals and hacktivists. Increasing the effectiveness of cyber-defensive systems is already a must and it will become more important than ever if we need, and want, to live in such technologically centered cities.

## **9.6.8 Contributions to the EU CyberSecurity Strategy for the Digital Decade**

### **9.6.8.1 Resilient infrastructure and critical services**

The EU's forthcoming new Network and Information Systems (NIS) Directive will aim to improve cyber resilience of all sectors relevant to the function of the economy and society, including both public and private sectors. These sectors are said to include at least energy, transport and health. Smart Cities have a close relationship with all of them:

- As previously discussed in this vertical, many digital solutions applied in Smart Cities are aimed at efficient usage of resources, including energy management
- Another core concept in Smart Cities is smart mobility, achieving safer, more comfortable and efficient transportation.
- The concept of Smart Cities also has a great impact in the health sector. Health IoT devices are increasingly prominent, and the data they provide are very useful for health services and research but need to be managed carefully. Other impacts include better emergency responses and indirect benefits due to environmental improvements (e.g., air pollution control).

Also, we remark that the list of sectors explicitly included on the Strategy are not exhaustive. The critical sectors finally identified will probably include other sectors related to this vertical. In fact, Smart Cities themselves are a core concept of future development on the digital world and technological societies. The work on this vertical has a direct impact on increasing security and privacy in Smart Cities. This will be critical to ensure the resilience the infrastructure, and to ensure the viability of these solutions, as citizens civil rights regarding privacy must be protected, which is not a trivial task in hyperconnected scenarios like Smart Cities.

### **9.6.8.2 Building a European Cyber Shield**

As remarked in the EU CyberSecurity Strategy document, the spread of connectivity and the growing sophistication of cyberattacks make Information Sharing and Analysis Centres, invaluable, as they allow the cyber threat information exchange between stakeholders necessary to defend against cybercrime. Smart Cities are a multi-stakeholder environment that also has the same requirements, especially if we consider the connectivity between different cities. The work done in establishing secure methods for communication and information sharing in Smart Cities will be closely related to the necessary tools for the consecution of the European Cyber Shield.

Additionally, even if not the main focus of this vertical, part of its work has focused on trusted and privacy-preserving sharing of cyber-threat data in the context of Smart Cities. With this, we aim to provide a key tool for protecting the heterogeneous environments (both in terms of technologies, and in terms of public and private entities involved) of Smart Cities, as well as establishing collaboration between security professionals in order to protect the vast attack surfaces of the digitalized world.

### **9.6.8.3 An ultra-secure communication infrastructure**

This vertical does not directly contribute to this dimension.

### **9.6.8.4 Securing the next generation of broadband mobile networks**

This vertical does not directly contribute to this dimension.

### **9.6.8.5 An Internet of Secure Things**

Smart cities are closely related to IoT scenarios. The growth of these scenarios also implies a proliferation in the number and variety of devices interacting with each other and sharing data of different nature and relevance. The protection of devices and the data they handle is particularly important. This vertical focuses on improving IoT scenarios through the application of different technologies that affect different strata of a Smart City. While this project has not focused on device certification or their lifecycles, other core topics for achieving an internet of secure things have been addressed.

Authentication based on eIDAS or privacy-preserving Attribute-Based Credentials are two examples of technologies that help to improve the security and privacy characteristics of the elements involved. In addition, Smart Cities also suffer from low trustworthiness, as there are many heterogeneous devices and services, which makes it more difficult to establish trust relationships. This vertical integrates DLT technologies to increase and improve those trust levels in a structural way. Also, the inclusion of MISP also improves CTI data sharing, increasing reactivity to threats in this scenario. Finally, the advances on communication and enforcement of regulations like GDPR are key to increase the *transparency* and applicability of security solutions. Thus, the security and privacy mechanisms developed by this vertical for the Smart City infrastructures can have a strong impact on the achievement of a secure internet of things.

### **9.6.8.6 Greater global Internet security**

This vertical does not directly contribute to this dimension.

### **9.6.8.7 A reinforced presence in the technology supply chain**

This vertical does not directly contribute to this dimension.

### **9.6.8.8 A Cyber-skilled EU workforce**

The GENOA demonstrator has the direct objective of increasing the cyber awareness of the municipality's civil servants, spreading the social engineering competencies in order to pay the way for an aware approach to this issue.

### **9.6.8.9 EU leadership on standards, norms and frameworks in cyberspace**

This vertical does not directly contribute to this dimension.

### **9.6.8.10 Cooperation with partners and the multi-stakeholder community**

This vertical does not directly contribute to this dimension.

### **9.6.8.11 Strengthening global capacities to increase global resilience**

This vertical does not directly contribute to this dimension.

### 9.6.9 Sector-specific Dimensions

This vertical does not directly contribute to this dimension.

### 9.6.10 Summary of the dimensions and impact on the Roadmap

The dimension most relevant and with the biggest impact on the roadmap was obviously the COVID-19 pandemic. Every data process included the smart city's ones, needs to be enforced in order to allow people in lockdown to access remotely to the city's services. This affects the user rights and specific consent needs to be explicitly stated and collected. That's the new push felt by this vertical, together with the threats to the democracy explained in section **Error! Reference source not found.** and summarized with the increased vulnerabilities of emergency and security alert systems, followed by street video surveillance and smart traffic lights.

Other dimensions impacted by this vertical are:

- Resilient infrastructure and critical services
- Building a European Cyber Shield
- An Internet of Secure Things
- A Cyber-skilled EU workforce

### 9.6.11 Challenge 1: Trusted Digital Platform

SCs usually require a variety of services, systems and applications that share servers and resources. Thus, the platform needs to tie different protections together and ensure that there are no privacy leaks at any point. Additionally, a security platform should be deployable across the many disparate systems that compose the SC environment, maintaining the required level of trust. Finally, it should support on-premises, IaaS (infrastructure as a Service), SaaS and hybrid cloud environments, to ensure that no device or server remains unconnected.

#### Specific Research Goals:

- **Identify leaks and violations**, SC is a complex platform where several different services, systems and applications may be used. All the different entities may represent a security risk able to compromise the overall platform trust. Possible vulnerabilities identification, definition of countermeasures as well as the identification of the best combination of protection methodologies to be applied in order to assure and assess required level of security and privacy can be challenging. An accurate analysis of the available tools and solutions should be enhanced in order to automate the assessment procedure.
- **Guaranteeing portability and interoperability**, SC platform and related features should be portable and deployable across different systems and environments. In order to keep the required level of trust, different approaches and means should be considered during platform realization so as to assure the management of heterogeneous network and communication, integration of different systems and components, the adoption of IaaS, SaaS and hybrid cloud environments.

#### JRC Cybersecurity Domains:

- Data Security and Privacy

- Design, implementation, and operation of data management systems that include security and privacy functions;
- Anonymity, pseudonymity, unlinkability, undetectability, or unobservability;
- Privacy Enhancing Technologies (PET);
- Digital Rights Management (DRM);
- Identity Management
  - Protocols and frameworks for authentication, authorization, and rights management;
  - Privacy and identity management (e.g. privacy-preserving authentication);
- Incident Handling and Digital Forensics
- Network and Distributed Systems
  - Network security (principles, methods, protocols, algorithms and technologies);
  - Distributed Systems Security;
  - Managerial, procedural and technical aspects of network security;
  - Network layer attacks and mitigation techniques;
  - Secure distributed computations;
- Software and Hardware Security Engineering
  - Security and risk analysis of components compositions
  - Secure software architectures and design;
  - Security design patterns
  - Self-including self-healing, self-protecting, self-configuration systems; Self-healing systems
- Trust Management and Accountability

#### **JRC Sectorial Dimensions:**

- Energy
- Defence
- Safety and Security
- Transportation

#### **JRC Technologies and Use Cases Dimensions:**

- Information Systems
- Critical Infrastructures
- Hardware technology
- Protection of public spaces
- Industrial IoT and Control Systems
- Internet of Things, embedded systems, pervasive

### **9.6.12 Challenge 2: Cyber threat intelligence and analysis platform**

Information sharing, active defence and automation methods should be integrated into the SC platform. Thus, it is necessary to develop efficient methods to create, disseminate, and consume threat intelligence in a standardized, usable, and legal way. It is also necessary to adopt defence mechanisms that will increase the cyber adversary's cost and decrease the overall efficiency of the active cyber operation. In parallel, in order to make the solutions effective, automation should be considered, and solutions integrated into business workflow, governance and structure control.

#### **Specific Research Goals:**

- **Design and implement efficient methods to exploits threat intelligence**, with the support of advanced and innovative techniques such as information sharing, active defence and automation methods.
- **Create common knowledge** based on data and information collected. This has the purpose of defining a standardized, usable, and legal background useful for: improving the performance of SCs; identifying and predicting possible cyber-attacks and vulnerabilities; supporting a continuous learning processes; developing efficient and efficacious defence mechanisms.
- **Develop and integrate solutions able to automatically enforce the defence mechanisms**. In order to increase the effectiveness of defence mechanisms, their integration into the business workflow, governance and structure control of the SC is challenging aspect.

### JRC Cybersecurity Domains:

- Human Aspects
  - Accessibility;
  - Usability;
  - Human-related risks/threats (social engineering, insider misuse, etc.)
  - Enhancing risk perception;
  - User acceptance of security policies and technologies;
  - Automating security functionality;
  - Privacy concerns, behaviours, and practices;
  - Human aspects of trust;
- Legal Aspects
  - Legal and societal issues in information security (e.g. identity management, digital forensics, cybersecurity litigation).
- Network and Distributed Systems
  - Distributed systems security analysis and simulation;
  - Distributed consensus techniques;
  - Secure distributed computations;
  - Network interoperability;
  - Secure system interconnection;
- Security Management and Governance
  - Threats and vulnerabilities modelling;
  - Managerial aspects concerning information security;
  - Assessment of information security effectiveness and degrees of control;
  - Governance aspects of incident management, disaster recovery, business continuity;
- Trust Management and Accountability

### JRC Sectorial Dimensions:

- Energy
- Defence
- Safety and Security
- Transportation

### JRC Technologies and Use Cases Dimensions:

- Artificial intelligence;

- Big Data;
- Blockchain and Distributed Ledger Technology (DLT);
- High-performance computing (HPC);
- Information Systems
- Critical Infrastructures
- Industrial IoT and Control Systems
- Internet of Things, embedded systems, pervasive systems
- Operating Systems;

### 9.6.13 Challenge 3: Cyber competence and awareness program

In order to improve the security level of SC, knowledge about possible risks and HW/SW attacks, as well as techniques such as encryption, anonymity and access control, should be improved. Thus, from one side, software engineers should be trained and informed about the possible security vulnerabilities and current technical solutions; from the other, end users should be informed about the security and privacy risks they could face and the correct security behaviour they should apply.

#### Specific research goals:

- **Collect and describe the possible HW/SW cyber-attacks**, so as to create a basic knowledge to be exploited by software engineering for: understanding the possible cyber risks; identifying the vulnerabilities of the platform and its components; managing the hidden and underestimated risks; deriving threats and complex attacks.
- **Develop an evidence-based and scenario-based risk database**, where the most commonly encountered cybersecurity incidents, attacks and scenarios are collected. This with the purpose of improving the software engineering learning processes as well as their ability in problem and case solving.
- **Collect and describe the most common SC security and privacy risks**. This information can be exploited for: training and informing the end users about the possible issues they could face during the usage of the SC platform; focusing the software engineering on possible recovery and security mechanisms to be adopted.

#### JRC Cybersecurity Domains:

- Assurance, Audit, and Certification
- Education and Training
  - Higher Education;
  - Professional training;
  - Cybersecurity-aware culture (e.g. including children's' education);
  - Cyber ranges, Capture the Flag, exercises, simulation platforms, educational/training tools, cybersecurity awareness;
  - Education methodology;
  - Vocational training.
- Human Aspects
  - Human-related risks/threats (social engineering, insider misuse, etc.)
  - Socio-technical security;
  - Enhancing risk perception;
  - User acceptance of security policies and technologies;
  - Transparent security;

- Cyber psychology;
- Human perception of cybersecurity;
- Capability maturity models (e.g. assessment of capacities and capabilities).
- Software and Hardware Security Engineering
- Trust Management and Accountability

### JRC Sectorial Dimensions

- Energy
- Defence
- Safety and Security
- Transportation

### JRC Technologies and Use Cases Dimensions:

- Critical Infrastructure Protection (CIP);
- Protection of public spaces;
- Disaster resilience and crisis management;
- Hardware technology (RFID, chips, sensors, networking, etc.)
- Human Machine Interface (HMI);
- Industrial IoT and Control Systems (e.g. SCADA and Cyber Physical Systems – CPS);
- Information Systems;
- Internet of Things, embedded systems, pervasive systems;
- Operating Systems;

## 9.6.14 Challenge 4: Privacy by design

Privacy by design encompasses seven principles that should be followed [Cavoukian 2019]: proactive privacy protection instead of remedial action after privacy violations have happened; privacy as the default setting; privacy embedded into the design; full functionality with full privacy protection; privacy protection through the entire lifecycle of the data; visibility and transparency; and respect for user privacy. Solutions for incorporating these principles into the design of new systems are needed. In parallel, data minimization approaches should be considered as a best practice for the adoption of privacy by design.

### Specific Research Goals:

- ***Ensuring the privacy by design principle in the SC platform.*** This research goal involves the integration of the privacy principle during the design of the architectures and systems used inside the SC environment. This includes: the identification of the possible privacy violations, attacks, accidents and threats that could be encountered during the SC operation stage; the definition of possible privacy principles and counter measures; the definition of the procedures for integrating privacy principles and recovery actions into the design of new systems.
- ***Design and demonstrate the privacy principles including integrity and confidentiality aspects.*** Considering the peculiarities and the complexity of the Smart City environment it is crucial to have specific solutions and facilities for demonstrating the privacy principle compliance.

### JRC Cybersecurity Domains:

- Data Security and Privacy
- Human Aspects

- Accessibility;
- Usability;
- Human-related risks/threats (social engineering, insider misuse, etc.)
- Enhancing risk perception;
- Privacy concerns, behaviours, and practices;
- Human aspects of trust;
- Human perception of cybersecurity;
- Identity Management
  - Protocols and frameworks for authentication, authorization, and rights management;
  - Privacy and identity management (e.g. privacy-preserving authentication);
  - Identity management quality assurance;
- Legal Aspects
  - Cybercrime prosecution and law enforcement;
  - Intellectual property rights;
  - Cybersecurity regulation analysis and design;
  - Legal and societal issues in information security (e.g. identity management, digital forensics, cybersecurity litigation).
- Network and Distributed Systems
  - Privacy-friendly communication architectures and services (e.g. Mix-networks, broadcast protocols, and anonymous communication);
- Security Management and Governance
  - Compliance with information security and privacy policies, procedures, and regulations;
  - Privacy impact assessment and risk management;
  - Processes and procedures to ensure device end-of-life security and privacy (e.g. IT waste management and recycling);
- Software and Hardware Security Engineering
  - Privacy by design.
- Trust Management and Accountability
  - Semantics and models for security, accountability, privacy, and trust;
  - Trust and privacy;

#### **JRC Sectorial Dimensions:**

- Energy
- Defence
- Safety and Security
- Transportation

#### **JRC Technologies and Use Cases Dimensions:**

- Industrial IoT and Control Systems (e.g. SCADA and Cyber Physical Systems – CPS);
- Information Systems;
- Blockchain and Distributed Ledger Technology (DLT);
- Internet of Things, embedded systems, pervasive systems;
- Mobile Devices;
- Operating Systems;
- Vehicular Systems (e.g. autonomous vehicles);

### 9.6.15 Challenge 5: Cyber response and resilience

All the solutions adopted for increasing security in SCs need to be effective in terms of volume, velocity, and variety of network traffic. Additionally, challenges such as network heterogeneity, high availability and scalability, and dynamic security policies of SCs should be also taken into consideration in designing possible solutions. If response measures and resilience to cyber threats are made an essential part of SC design, a higher security level will benefit the overall framework, governance, and business.

#### Specific Research Goals:

- ***Ensuring the performance of SCs.*** The peculiarities and complexity of the SCs rise different performance challenges in terms of volume, velocity, and variety of network traffic. Specific solutions for assessing SC performance, availability, scalability and security should be enforced taking in consideration also the heterogeneity of the systems and resources involved.
- ***Ensuring the resilience of the SCs.*** This research goal involves the development of novel features for ensuring resilience to unwanted events, such as deliberate attacks, accidents, or naturally occurring threats, without exhibiting complete failure of critical operations. In addition, novel methodologies and tools need to be developed to allow the fast recovery of SC systems.

#### JRC Cybersecurity Domains:

- Identity Management
  - Identity management quality assurance;
- Incident Handling and Digital Forensics
  - Vulnerability analysis and response;
  - Resilience aspects;
  - Anti-forensics and malware analytics;
- Network and Distributed Systems
  - Network security (principles, methods, protocols, algorithms and technologies);
  - Distributed systems security;
  - Requirements for network security;
  - Distributed systems security analysis and simulation;
  - Distributed consensus techniques;
  - Secure distributed computations;
  - Network interoperability;
  - Secure system interconnection;
- Security Measurements
  - Security analytics and visualization;
  - Security metrics, key performance indicators, and benchmarks;
  - Validation and comparison frameworks for security metrics;
  - Measurement and assessment of security levels.
- Software and Hardware Security Engineering
  - Security requirements engineering with emphasis on identity, privacy, accountability, and trust;
  - Runtime security verification and enforcement;
  - Quantitative security for assurance;
  - Self-\* including self-healing, self-protecting, self-configuration systems;

- Theoretical Foundations
  - Formal specification, analysis, and verification of software and hardware;
  - Formal verification of security assurance;

#### JRC Sectorial Dimensions

- Energy
- Defence
- Safety and Security
- Transportation

#### JRC Technologies and Use Cases Dimensions:

- Information Systems
- Critical Infrastructures
- Hardware technology
- Protection of public spaces
- Industrial IoT and Control Systems
- Internet of Things, embedded systems, pervasive
- Satellite systems and applications;
- Vehicular Systems (e.g. autonomous vehicles);

### 9.6.16 Challenge 6: End user trusted data management

This encompasses different activities: i) assuring transparency, i.e. openly communicating what data is collected, what data is stored, how it is processed, who it is shared with, and how it is protected; ii) managing consent and control, i.e. making end users aware of the data held about them; giving end users the right to view, update and delete their data, and ensuring that data is handled according to each user's privacy settings; iii) implementing auditing and accountability procedures, i.e. holding the city accountable for the use of end users' data, compliance with privacy policies and the prompt detection of misbehaviour.

#### Specific Research Goals

- ***Design and implement means and measures assuring secure and transparent data collection and communications.*** The solutions should take into consideration the environmental peculiarities of SCs (network availability and the communication cost) as well as challenges relative to data storage and processing. Additionally, the solutions need to be scalable and redundant.
- ***Develop and integrate access and usage control mechanisms able to managing the users consent and rights.*** The purpose is, from one side, to assure the correct and conform data access management; and from the other, to make the end users aware of their rights and privacy settings. This research goal include also data usage control and data provenance approaches, from a conceptual and technological point of view to facilitate a secure and trustworthy personal data exchange between different services.
- ***Design and implement auditing and accountability procedures.*** The purpose is to: precisely define the privacy policies; implement auditing and accountability features; provide means for assuring compliance with privacy policies; define features for the prompt detection of misbehaviour. Solutions that assure that the communication are not exposed to intruders and not compromised are also challenging.
- ***Self-sovereign identity.*** The notion of self-sovereign identity has emerged in the past few years and the road toward actual self-sovereign identity is at the early stages. This research goal is about

understanding how to adopt and implement a digital identity system that provides full control and autonomy to the individuals.

### **JRC Cybersecurity Domains:**

- Assurance, Audit, and Certification
- Data Security and Privacy
  - Privacy requirements for data management systems;
  - Design, implementation, and operation of data management systems that include security and privacy functions;
  - Anonymity, pseudonymity, unlinkability, undetectability, or unobservability;
  - Data integrity;
  - Privacy Enhancing Technologies (PET);
  - Digital Rights Management (DRM);
  - Data usage control.
- Human Aspects
  - Accessibility;
  - Usability;
  - Human-related risks/threats (social engineering, insider misuse, etc.)
  - Socio-technical security;
  - Enhancing risk perception;
  - User acceptance of security policies and technologies;
  - Privacy concerns, behaviours, and practices;
  - Computer ethics and security;
  - Transparent security;
  - Human aspects of trust;
  - Human perception of cybersecurity;
- Legal Aspects
  - Legal and societal issues in information security (e.g. identity management, digital forensics, cybersecurity litigation).
- Security Management and Governance
  - Compliance with information security and privacy policies, procedures, and regulations;
  - Privacy impact assessment and risk management;
  - Processes and procedures to ensure device end-of-life security and privacy (e.g. IT waste management and recycling);
- Trust Management and Accountability

### **JRC Sectorial Dimensions**

- Energy
- Defence
- Safety and Security
- Transportation

### **JRC Technologies and Use Cases Dimensions:**

- Critical Infrastructure Protection (CIP);
- Industrial IoT and Control Systems (e.g. SCADA and Cyber Physical Systems – CPS);

- Information Systems;
- Blockchain and Distributed Ledger Technology (DLT);
- Internet of Things, embedded systems, pervasive systems;
- Mobile Devices;
- Operating Systems;
- Vehicular Systems (e.g. autonomous vehicles);

### 9.6.17 Challenge 7: Interoperability between legacy and new systems

Every new system or application integrated into the SC environment may represent a potential gate for attackers. Actually, the level of interoperability between legacy and new systems could represent the level of criticality of the overall system: the more connected the network, the more vulnerabilities there are for attackers to exploit. Possible solutions could be: provide validated and precise interoperability recommendations and specification; define specific governance; provide on line verification and validation means for promptly identifying a possible security risk. In parallel, data should be encrypted both at rest and in transit. Indeed, encrypting prevents attackers from misusing the data in case of a breach.

#### Related Research Goals:

- **Define interoperability specifications and risks**, so as to provide useful guidelines and precise interoperability recommendations for validating and assessing the required level of interactions. The identification of the possible security risks strictly connected with the integration of new system should also be defined in order better focus the validation and verification steps.
- **Guaranteeing interoperability**, SCs integrate different systems and applications that should work in collaboration. Specific verification and validation approaches and means should be considered so as to assure the interoperability between legacy and new systems. Similarly, mechanisms aimed to enable privacy-preserving and data protection should mainly focus on standards and approaches widely employed nowadays, in order to further ensure interoperability among involved entities.

#### JRC Cybersecurity Domains:

- Cryptology (Cryptography and Cryptanalysis)
- Identity Management
  - Identity management quality assurance;
- Incident Handling and Digital Forensics
  - Theories, techniques and tools for the identification, collection, attribution, acquisition, analysis and preservation of digital evidence (e.g. code authorship and attacker identification, provenance assurance, digital evidence correlation, digital evidence triage);
  - Vulnerability analysis and response;
  - Coordination and information sharing in the context of cross-border/organizational incidents.
- Network and Distributed Systems
  - Network interoperability;
  - Secure system interconnection;
  - Privacy-friendly communication architectures and services (e.g. Mix-networks, broadcast protocols, and anonymous communication);
- Security Management and Governance
  - Assessment of information security effectiveness and degrees of control;

- Identification of the impact of hardware and software changes on the management of Information Security
- Privacy impact assessment and risk management;
- Capability maturity models (e.g. assessment of capacities and capabilities).
- Security Measurements
  - Validation and comparison frameworks for security metrics;
- Software and Hardware Security Engineering
  - Security design patterns;
  - Secure programming principles and best practices;
  - Security support in programming environments;
  - Refinement and verification of security management policy models;
  - Runtime security verification and enforcement;
  - Security testing and validation;
  - Vulnerability discovery and penetration testing;
  - Quantitative security for assurance;
  - Model-driven security and domain-specific modelling languages;
  - Fault injection testing and analysis;
  - Cybersecurity and cyber-safety co-engineering;
- Theoretical Foundations
  - Information flow modeling and its application to confidentiality policies, composition of systems, and covert channel analysis;
  - Formal verification of security assurance;

#### **JRC Sectorial Dimensions**

- Energy
- Defence
- Safety and Security
- Transportation

#### **JRC Application and Technology Dimensions**

- Critical Infrastructure Protection (CIP);
- Industrial IoT and Control Systems (e.g. SCADA and Cyber Physical Systems – CPS);
- Information Systems;
- Internet of Things, embedded systems, pervasive systems;
- Mobile Devices;
- Operating Systems;
- Vehicular Systems (e.g. autonomous vehicles);

### **9.6.18 Challenge 8: Cyber fault/failure detection and prevention**

An important part of SC development is fault/failure detection and prevention to ensure that the design and implementation of the overall platform fulfil its security and privacy requirements. A possible solution is to adopt specific testing and verification approaches for finding information leaks and possible threats targeting security and privacy vulnerabilities. Fault/failure detection and prevention testing are core engineering activities that should be targeted in all the phases and stages of the SC specification, development, integration, and delivery cycle. For this model-based testing, automated assessment and

configuration (generation of drivers, stubs, and intercepting proxies), automated dependability assessment and planning should be taken in consideration. Investigated methods should also include security and privacy testing as well as the fault-tolerance analysis and reconfigurability of systems, applications, and infrastructure so to check the CS vulnerabilities and enhance their security and trust.

#### Related research goals:

- **Identify the verification and validation approaches.** Depending on the specific security and privacy vulnerabilities different testing and verification approaches could be applied. In order to reduce the verification and validation effort and time, and to assure an effective and efficient fault/failure detection activity, the best combination of different validation and verification methodologies need to be identified.
- **Define a common fault/failure catalogue.** Based on the results collected during the verification and validation activity, a supporting catalogue able to classify the most frequently encountered faults/failures as well as to collect the recovery performed activities should be defined. This can be a baseline for improving the efficiency and effectiveness of the validation and verification approaches and an important support for the subsequent faults/failures recovery and repair.
- **Focus on individual behaviours:** The existing models, methods, and tools for the verification and testing of test should be extended and integrated for including individual behaviours or collective behaviour of a SC users.
- **Trust management:** in order to control the trust dynamics in a SC a multi-level trust management able to take in consideration the trust outcomes both at system and individual level should be considered.

#### JRC Cybersecurity Domains:

- Security Management and Governance
  - Risk management, including modelling, assessment, analysis and mitigations;
  - Threats and vulnerabilities modelling;
  - Attack modelling, techniques, and countermeasures (e.g. adversary machine learning);
  - Assessment of information security effectiveness and degrees of control;
  - Techniques to ensure business continuity/disaster recovery;
  - Privacy impact assessment and risk management;
  - Capability maturity models (e.g. assessment of capacities and capabilities).
- Security Measurements
  - Security analytics and visualization;
  - Security metrics, key performance indicators, and benchmarks;
  - Validation and comparison frameworks for security metrics;
  - Measurement and assessment of security levels.
- Software and Hardware Security Engineering
- Theoretical Foundations

#### JRC Sectorial Dimensions

- Energy
- Defence
- Safety and Security
- Transportation

#### JRC Application and Technology Dimensions

- Critical Infrastructure Protection (CIP);

- Industrial IoT and Control Systems (e.g. SCADA and Cyber Physical Systems – CPS);
- Information Systems;
- Internet of Things, embedded systems, pervasive systems;
- Mobile Devices;
- Operating Systems;
- Vehicular Systems (e.g. autonomous vehicles);

### 9.6.19 Challenge 9: Logging and monitoring

Logging and monitoring activity is an essential asset for controlling and managing different SC due to stringent characteristics such as: dependability requirements, decentralized management, loose coupling and dynamic deployment of independent systems. Runtime logging and monitoring refers to the capability of an application to track and trace the state of objects, discover information regarding its past states and potentially estimate future states. In [KEH 2014], the authors give a taxonomy and a comprehensive survey of numerous monitoring tools, approaches and mechanisms available for large scale cloud environments.

In SC, large quantities of data are captured and exchanged across the platform. Thus, online logging and monitoring solutions allow continuous searching for potential indicators of compromised signals or services, as well as potential threats.

Thus, the classical approaches used for security and privacy logging and monitoring in the broader sense, can be nowadays integrated into the SC environment so as to rapid prototyping migration from virtual to real (parts of the) system, as well as to monitor and control resources and data management and protection. In practice these can help both the security and privacy of the running system and its off-line management through its model, allowing also a smooth migration from a prototype system, relying on a set of virtual nodes and devices, possibly automatically generated from the system model, to the real system.

Logging and monitoring also allow an SC to demonstrate that it complies with its privacy policies. In addition, security measures should be specified and implemented in the platform to immediately isolate and solve potential vulnerabilities.

#### Related Research Goals:

- ***Ensuring online logging and monitoring solutions.*** This research goal involves the development of logging and monitoring solutions to be integrated into the SC environment in order to: have a smart tracking of behaviour of the SC by means of the collation of specific KPIs; assure prompt alerts in case unwanted events (attacks, accidents, KPI violations, or failures); demonstrate SC compliance with its privacy policies.
- ***Ability to quickly adapt to security threats.*** This research goal entails the development and implementation of monitoring techniques, supported by specific rules and KPIs, that can enable SCs to quickly react to attacks and apply proper mitigation controls. In addition, novel methodologies and tools need to be developed to allow the fast recovery in case of fault and failures.
- ***Increasing security and privacy*** The increasing demand for security and privacy from final consumers sets high requirements for well-structured traceability systems. Additionally, mining techniques employed in these applications have to be efficient in terms of space usage and per-item processing time while providing a high quality of answers to aggregate monitoring queries, such as finding surprising levels of a data stream, detecting bursts, and to similarity queries, such as

detecting correlations and finding interesting patterns. Provenance-based traceability provides a mean to capture and query events occurred in the past to understand how and why they took place.

- ***Self-adaptive logging and monitoring***: Providing monitoring and logging facilities able to continuously (self) adapt themselves to the evolving SC environment and to manage and analyse huge quantities of data. There is also the need of enhancing the existing monitoring approaches for promptly rising warnings and detecting failures as well as for SC reconfiguration and dependability compliance.
- ***Improved solutions*** Logging and monitoring systems should be conceived so as to be able to capture, analyse and visualize complex events so as to detect critical problems, failures and security and privacy vulnerabilities.

●

### **JRC Cybersecurity Domains:**

- Assurance, Audit, and Certification
- Network and Distributed Systems
  - Distributed systems security;
  - Managerial, procedural and technical aspects of network security;
  - Network layer attacks and mitigation techniques;
  - Network attack propagation analysis;
  - Distributed systems security analysis and simulation;
  - Network interoperability;
  - Secure system interconnection;
- Security Management and Governance
  - Threats and vulnerabilities modeling;
  - Attack modeling, techniques, and countermeasures (e.g. adversary machine learning);
  - Managerial aspects concerning information security;
  - Assessment of information security effectiveness and degrees of control;
  - Techniques to ensure business continuity/disaster recovery;
- Security Measurements
- Software and Hardware Security Engineering
  - Security support in programming environments;
  - Security documentation;
  - Runtime security verification and enforcement;
  - Quantitative security for assurance;
  - Self-\* including self-healing, self-protecting, self-configuration systems;

### **JRC Sectorial Dimensions**

- Energy
- Defence
- Safety and Security
- Transportation

### **JRC Application and Technology Dimensions**

- Critical Infrastructure Protection (CIP);
- Industrial IoT and Control Systems (e.g. SCADA and Cyber Physical Systems – CPS);
- Information Systems;
- Internet of Things, embedded systems, pervasive systems;

- Mobile Devices;
- Operating Systems;
- Vehicular Systems (e.g. autonomous vehicles);

### 9.6.20 Challenge 10: Information security and operational security

As a matter of fact, in the last years the most part of existing SC systems has been connected to the Internet, due to the ever increasing coverage of Internet connectivity. It is obvious that, if on the one hand this connectivity enables the provision of new and better services, on the other hand, it introduces new security and privacy risks of unauthorized access to and usage of such systems. In order to prevent privacy violations and erroneous or malicious uses, security solutions that allow to address aspects related to privacy and data protection should be provided. More in detail, the integration of mechanisms to control access shared data is required, so that only authorized entities are able to retrieve them. Similarly, considering mechanisms to guarantee privacy-preserving of involved entities during the whole data sharing process is needed. Thus, SCs need to be protected by proper security mechanisms, such as authentication and authorization of users accessing the system, protection (e.g. encryption of files and data by ransomware) of data at rest and of communications, system availability and auditability, and so on. It is straightforward that such mechanisms must be embedded in the architecture already from the design phase, because adding them to an already defined architecture could be inefficient or could require disruptive modifications of the architecture itself.

#### Related research goals:

- ***Design and implement measures to protect against ransomware, and malware in general***, that might compromise the SC infrastructure. Methodologies and tools should be also adopted to identify and assess the possible risks deriving from threats and attacks.
- ***Design and demonstrate a trust infrastructure that facilitates preservation of integrity and confidentiality aspects***. As the common threat is the encryption of files and data by ransomware, it is crucial to have solutions that assures that this information is not exposed to intruders and/or compromised.
- ***Design and integrate security approaches with the aim of dealing with privacy and data protection aspects***. The inclusion of mechanisms aimed to protect shared information should be considered, in order to control data access and avoid unauthorized accesses. Additionally, privacy-preserving techniques need to be adopted, in order to protect privacy of involved entities.
- ***Evaluating of security and privacy***: Security and privacy are crucial for SC systems, that could also have a relevant impact on safety. Many security incidents are due by design or implementation flaws. An evaluation of security aspects of SC systems is crucial for both the system design and development processes, since performing such security evaluation phase, vulnerabilities can be detected and solved directly at design and/or development time. Moreover, the security evaluation could be performed even periodically on existing (i.e. already designed and implemented) SC in order to check them against new threats that were not known at design and development time.
- ***Enhancing existing solutions***. For SC is therefore important to enhance the existing security solutions in order to check the SC against new threats that were not known at design and development time and may depend on Hardware and Software interactions. Moreover, dependencies between security and privacy properties and functional ones so to provide integrated solutions able to solve both of them should be also considered

#### JRC Cybersecurity Domains:

- Assurance, Audit, and Certification
- Cryptology (Cryptography and Cryptanalysis)
- Data Security and Privacy
  - Anonymity, pseudonymity, unlinkability, undetectability, or unobservability;
  - Data integrity;
  - Privacy Enhancing Technologies (PET);
  - Risk analysis and attacks with respect to de-anonymization or data re-identification (e.g. inference attack);
  - Data usage control.
- Incident Handling and Digital Forensics
  - Incident analysis, communication, documentation, forecasting (intelligence based), response, and reporting;
  - Theories, techniques and tools for the identification, collection, attribution, acquisition, analysis and preservation of digital evidence (e.g. code authorship and attacker identification, provenance assurance, digital evidence correlation, digital evidence triage);
  - Vulnerability analysis and response;
  - Anti-forensics and malware analytics;
- Network and Distributed Systems
  - Network layer attacks and mitigation techniques;
  - Network attack propagation analysis;
  - Fault tolerant models;
- Security Management and Governance
  - Threats and vulnerabilities modeling;
  - Attack modeling, techniques, and countermeasures (e.g. adversary machine learning);
  - Assessment of information security effectiveness and degrees of control;
  - Identification of the impact of hardware and software changes on the management of Information Security
  - Standards for Information Security;
- Software and Hardware Security Engineering
  - Runtime security verification and enforcement;
  - Security testing and validation;
  - Vulnerability discovery and penetration testing;
  - Quantitative security for assurance;
  - Intrusion detection and honeypots;
  - Malware analysis including adversarial learning of malware;
  - Attack techniques (e.g. side channel attacks, power attacks, stealth attacks, advanced persistent attacks, rowhammer attacks);
  - Fault injection testing and analysis;
- Theoretical Foundations
  - Information flow modeling and its application to confidentiality policies, composition of systems, and covert channel analysis;

### JRC Sectorial Dimensions

- Energy
- Defence

- Safety and Security
- Transportation

### JRC Application and Technology Dimensions

- Critical Infrastructure Protection (CIP);
- Industrial IoT and Control Systems (e.g. SCADA and Cyber Physical Systems – CPS);
- Information Systems;
- Internet of Things, embedded systems, pervasive systems;
- Mobile Devices;
- Operating Systems;

Vehicular Systems (e.g. autonomous vehicles);

## 9.7 Mapping of the Challenges to the Big Picture

The challenges above-mentioned were selected from the big picture, with the aim of defining the most important and urgent ones:

**Challenge 1:** Trusted Digital Platform. A digital platform enables citizen-centric services for all citizens delivering seamless services. In order for the digital platform to be used, it must be trusted by citizens, i.e. it must guarantee the protection of personal data

**Challenge 2:** Cyber threat intelligence and analysis platform. One of the enablers mentioned in the big picture has to provide specific threat intelligence and analysis.

**Challenge 3:** Cyber competence and awareness program. As clear by most of the recent cyberattacks, the human factor is one of the most used attack strategies by the attackers. Too often they find the way to bypass the countermeasures through an employee lacking the necessary skills to deal with a threat or an inattentive user.

**Challenge 4:** Privacy by design. This is a must when new public services use citizens' data. This challenge gained more relevance after the GDPR entry into force.

**Challenge 5:** Cyber response and resilience. The new (and many) vulnerable surfaces mentioned for challenge 2 are the main reason behind the need for a prompt response to the attacks and the creation of a resilient infrastructure.

**Challenge 6:** End user trusted data management. This challenge is due to address one of the main objectives behind an SC platform: without citizens' trust in the data collection and processing, nobody would like to publish and use services or data from an untrusted space.

**Challenge 7:** Interoperability between legacy and new systems. This challenge is necessary for guaranteeing an interoperable digital platform based on open standards and technical specifications.

**Challenge 8:** Cyber fault/failure detection and prevention. The identification and classification of the most frequently encountered faults and failures during the SC development can assure an appropriate security and privacy level and improve user trustworthiness in the SC platform itself.

**Challenge 9:** Logging and monitoring: This challenge is important for tracing the users (citizens, tourists and NGOs) and platform behaviour during the online operation. The analysis of collected data can provide insights about the security threats and vulnerabilities encountered and suggest possible counter measures.

**Challenge 10:** Information security and operational security. This challenge is necessary for a citizen-centric approach where users are made confident about the security level provided by the SC infrastructure.

## 9.8 Methods, Mechanisms, and Tools

An ever-growing number of methods, mechanisms and tools are being developed to meet the above challenges with increasing efficiency and effectiveness. The table below shows the tools that deal with the challenges of SC. In bold the ones that could be included in the SC demonstrator.

Table 10: Challenges identified in the Smart Cities Vertical and Tools needed to address them.

Challenge	Tools required	Tools contemplated for Smart Cities	Tools/Methods that need to be addressed
Challenge 1	Trusted Digital Platform	<ul style="list-style-type: none"> <li>● <b>SPeIDI</b> (D3.1, Section 5.1)</li> <li>● <b>Mobile p-ABC</b> (D3.1, Section 5.1)</li> <li>● <b>eiDASBrowser</b> (D3.1, Section 5.1)</li> <li>● DynSmaug (D3.1, Section 5.4)</li> <li>● VCUCIM (D3.1, Section 5.4)</li> <li>● EEVEHAC (D3.1, Section 5.5)</li> </ul>	Incident Handling and Digital Forensics Network and Distributed Systems Software and Hardware Security Engineering
Challenge 2	Cyber threat intelligence and analysis platform	<ul style="list-style-type: none"> <li>● <b>Threat Intelligence Integrator</b> (D3.1, Section 5.3)</li> </ul>	Legal Aspects Governance aspects of management, recovery, and continuity Information security
Challenge 3	Cyber competences and awareness program	<ul style="list-style-type: none"> <li>● <b>TO4SEE</b> (D5.2, Section 8.2.3.2)</li> </ul>	A campaign from the public administration to improve the cyber competences and awareness of the citizens will be useful.
Challenge 4	Privacy by design	<ul style="list-style-type: none"> <li>● <b>GENERAL_D</b> (D3.1, Section 5.1)</li> <li>● <b>PPIIdM</b> (D3.1, Section 5.1)</li> <li>● <b>PLEAK</b> (D3.1, Section 5.2)</li> <li>● <b>CaPe</b> (D5.2, Section 8.2.3.2)</li> </ul>	Trust Management and Accountability. The WP3 and WP5 tools cover 5 of the 7 seven “Privacy by Design” principles. The following ones need to be addressed beyond the project: <ul style="list-style-type: none"> <li>● full functionality with full privacy protection;</li> <li>● privacy protection through the entire lifecycle of the data.</li> </ul>
Challenge 5	Cyber response and resilience	<ul style="list-style-type: none"> <li>● <b>Briareos</b> (D3.1, Section 5.3)</li> <li>● <b>RATING</b> (D5.2, Section 8.2.3.2)</li> </ul>	Theoretical Foundations Identity Management

Challenge 6	End user trusted data management	<ul style="list-style-type: none"> <li>● <b>PPI</b>dM (D3.1, Section 5.1)</li> <li>● <b>DANS</b> (D3.1, Section 5.1)</li> <li>● <b>PLEAK</b> (D3.1, Section 5.2)</li> <li>● <b>CaPe</b> (D5.2, Section 8.2.3.2)</li> <li>● <b>ARGUS</b> (D3.11, Section 5.9)</li> <li>● <b>PTASC</b> (D3.11, Section 5.8)</li> </ul>	Data usage control Privacy concerns, behaviours, and practices Human aspects of trust User acceptance of security policies and technologies Auditing and accountability procedures
Challenge 7	Interoperability between legacy and new systems	<ul style="list-style-type: none"> <li>● <b>SPeIDI</b> (D3.1, Section 5.1)</li> <li>● <b>PTASC</b> (D3.11, Section 5.8)</li> <li>● <b>eIDASBrowser</b> (D3.1, Section 5.1)</li> </ul>	Legal Aspects Network and Distributed Systems Formal verification of security assurance Software and Hardware Security Engineering Theoretical Foundations
Challenge 8	Cyber fault/failure detection and prevention	<ul style="list-style-type: none"> <li>● <b>Briareos</b> (D3.1, Section 5.3)</li> <li>● <b>RATING</b> (D5.2, Section 8.2.3.2)</li> </ul>	Theoretical Foundations
Challenge 9	Logging and monitoring	<ul style="list-style-type: none"> <li>● <b>CaPe</b> (D5.2, Section 8.2.3.2)</li> </ul>	Auditing and accountability procedures for personal data management in compliance with GDPR
Challenge 10	Information security and operational security	<ul style="list-style-type: none"> <li>● <b>Mobile p-ABC</b> (D3.1, Section 5.1)</li> <li>● <b>DynSmaug</b> (D3.1, Section 5.4)</li> <li>● <b>VCUCIM</b> (D3.1, Section 5.4)</li> <li>● <b>EEVEHAC</b> (D3.1, Section 5.5)</li> </ul>	Network and Distributed Systems Software and Hardware Security Engineering

### 9.8.1 Integrated Security Risk Framework

From the EU perspective, ENISA provided many reports and guidelines about risk assessment, as well as establishing a specific working group within itself.<sup>487</sup> ENISA defines 3 phases for the risk assessment process: Identification of Risks, Analysis of Relevant Risks, and Evaluation of Risks. After the initial analysis of the context and objectives suggested by AgID, the 3 ENISA phases should be conducted, starting from generating a comprehensive list of sources of threats, risks and events that might have an impact on the achievement of each of the objectives identified previously. Secondly, the risk identification methodology has to be selected, and ENISA suggests the following techniques:

- team-based brainstorming where workshops can prove effective in building commitment and making use of different experiences;

<sup>487</sup> <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/working-group>

- structured techniques, such as flow charting, system design review, systems analysis, hazard and operability studies, and operational modeling;
- for less clearly defined situations, such as the identification of strategic risks, processes with a more general structure, such as “what-if” and scenario analysis, could be used.

When all the potential risks are identified, risk analysis is the phase where the level of the risk and its nature are assessed and understood. It involves:

- thorough examination of the risk sources;
- their positive and negative consequences;
- the likelihood that those consequences may occur and the factors that affect them;
- assessment of any existing controls or processes that tend to minimize negative risks or enhance positive risks.

A calculation combining impact and likelihood is used to assign a level to the risk and a value to its estimation. To perform this calculation, ENISA suggests using:

- past experience or data and records (e.g. incident reporting),
- reliable practices, international standards or guidelines,
- market research and analysis,
- experiments and prototypes,
- economic, engineering or other models,
- specialist and expert advice.

The last phase is the risk evaluation. During the risk evaluation phase, ENISA specifies that decisions have to be made concerning which risks need treatment and which do not, as well as concerning the treatment priorities. The decisions made are usually based on the level of risk, but may also be related to thresholds specified in terms of consequences (e.g. impacts), the likelihood of events, the cumulative impact of a series of events that could occur simultaneously.

Taking in to account these guidelines, in a concrete tentative of risk management, it is also well acknowledged that waterfall approaches to manage and mitigate risks are largely inadequate in evolving contexts, such as the one that characterizes the ICT infrastructures of SC. Iterative approaches, in turn, offer a much more flexible way to address cybersecurity needs, also taking into account time- and cost-related constraints. In this field, an adaptation of the well-known and consolidated Plan-Do-Check-Act (PDCA) cycle was proposed and successfully tested by the EU co-funded project COMPACT<sup>488</sup> to improve the resilience of local public administrations. The four phases of the Plan-Do-Check-Act cycle are:

1. **Plan:** Identify and analyse the problem through context establishment, risk assessment, risk treatment plan development and risk acceptance.

---

<sup>488</sup> Project co-funded by the European Commission under the Horizon 2020 Programme (GA n. 740712)

2. **Do:** Develop and test a potential solution, performing all the actions included in the risk treatment plan.
3. **Check:** Measure how effective the tested solution was and analyse whether it could be improved with continuous monitoring and a revision of the risk assessment and treatment in the light of incidents and changes of the context.
4. **Act:** Implement the improved solution fully. The “Act” phase becomes “**Adjust**”, in order to make evident that the actions carried out here are a concrete refinement of the solution, through any activity needed to maintain and improve the entire SC cyber-security management process.

This process enables LPAs to innovate their cyber security improvement process in compliance with the EN ISO/IEC 27001 and BS ISO/IEC 27005 standards [COMPACT 2018].

In July 2018, a new edition of ISO/IEC 27005 was published (the third), entitled “Information security risk management”. This represents an international standard that is nowadays well-known for assessing the risk related to information security. Therefore, like COMPACT, the CyberSec4Europe project will also start from a predefined process and will adapt it to the context of an SC. The main difference between the COMPACT context, focused on the LPA’s employees, and the CyberSec4Europe project is the presence of citizens as natural users of SC services.

To implement the PDCA cycle, a set of tools, methodologies and best practices will be used according to defined goals. The following image (Figure 28) introduces the four process steps, together with the related input and output, as well as the tools that may be helpful for implementing each one.

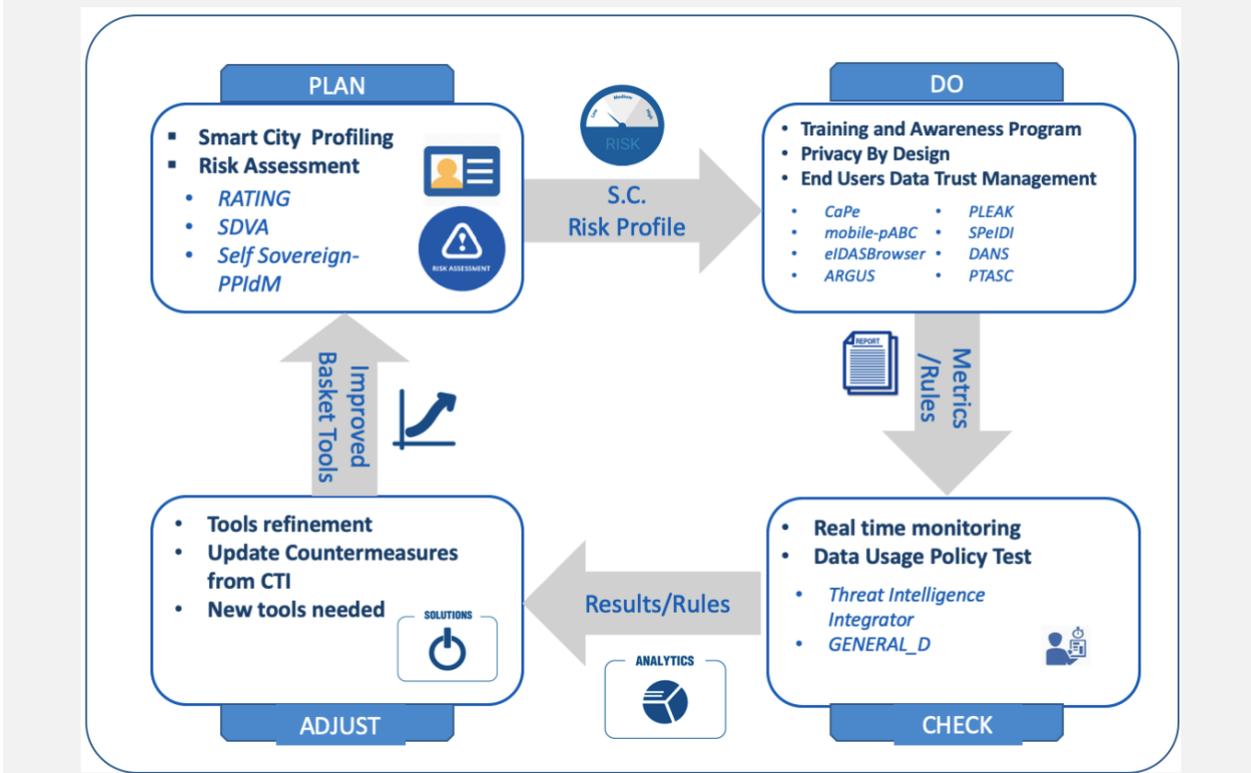


Figure 28: PDCA cycles for SC vertical

With the increase in integration between digital and physical worlds, SC need to identify and evaluate emerging risks and, especially, evaluate the cascading effects of a potential attack.

Nowadays, there are several methods and frameworks; among these, the NIST cyber security framework provides best-practices and guidelines for improving the cybersecurity of critical infrastructure<sup>489</sup> (in line with ISO31000 [ISO31000 2018]).

Following the NIST directive, risk assessment is part of the identification stage, whose aim is to establish the context, profile the infrastructure, identify assets and businesses to protect, evaluate impacts and highlight emerging risks associated with the infrastructure's vulnerabilities.

Regarding security measures for the protection of personal data, following a risk-based approach, ENISA has also provided guidelines<sup>490</sup> on how to assess risks related to data privacy during personal data processing and how to develop appropriate protective measures to prevent the loss of confidentiality, integrity and availability of data assets.

In the context of the SC demonstrator, the risk assessment and management activities will be addressed by using existing tools, and will include:

- Vulnerability estimation of the infrastructure's cyber posture, whose aim is to evaluate its cyber maturity model and highlight weaknesses and dangerous threats.
- Economic estimation of the loss, especially of intangible assets (such as digital data and reputation), by evaluating the intangible capital of the organization and the economic value of the intangible assets at risk.
- Risk scenarios, with a particular focus on the evaluation of cascading effects due to the possible attacks and their related costs.
- Evaluate the security of digital personal data operations, providing privacy risk assessments for data controllers and data processors. The aims are to establish the context of the data operation, understand and evaluate the impact, identify threats and evaluate the probability of their occurrence. Following the evaluation of the risk, the data processors and controllers can adopt technical and organizational security measures.
- Provide a cost-benefit analysis of cyber security investments to mitigate intolerable emergent risks
- Perform a penetration test by a phishing attack simulation, targeting all the civil servants of the municipality.

### 9.8.2 Cyber competences and awareness program

While companies try to deploy technical, physical and procedural security controls, these are ultimately operated and managed by people who can make mistakes and/or act maliciously, thus circumventing or disabling the actual controls. For this reason, the most successful attacks are those aimed at exploiting the weaknesses of people. International security best practices and standards require organizations to ensure

---

<sup>489</sup> <https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf>

<sup>490</sup> <https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing>

that an adequate level of security awareness is delivered to their staff. Training and awareness of operators is a key aspect in ensuring the security of systems. Several solutions and services help organizations to address the traditional weakest link of the chain: the human. Therefore, improving the level of cyber competence and awareness of people within an organization, and maintaining it at a high level, is a key challenge. This is even more important in SC contexts, where a large number of users, including citizens, has access to the infrastructure.

On the training side, organizations can count on a wide range of platforms specifically designed for educational and teaching purposes (e.g. Moodle). One important feature of these platforms is the possibility to manage and integrate training offered by different vendors. Standards are emerging in this regard, such as the xAPI, which allow for a formal definition of training offers, plans and results (using the learning record concept).

On the awareness side, approaches based on gamification are becoming mainstream. This because participation in security awareness activities is still seen by employees as a “dictated” activity, which requires setting aside personal time to do a company-related task. As such, it carries with it all the traditional work-related performance issues, including adequate management of the security awareness process to ensure people attend the required activities. In turn, providing security awareness training through a gamified environment has been proven to achieve better participation from people who will then learn by playing.

### 9.8.3 Privacy by design and end user trusted data management

Personal data is becoming a new economic “asset class”, a valuable resource for the 21<sup>st</sup> century that will reach all corners of society. A fundamental point in the creation of SC is the generation, analysis and sharing of large quantities of data. SC technologies capture data about people and places at all levels of privacy, and day by day they drastically expand the volume, range and granularity of the data being collected and processed.

However, this SC process puts individual privacy at risk, thus reducing individual trust.

The introduction in May 2018 of tighter regulations in the form of the General Data Protection Regulation – the EU’s ambitious new data protection law – should pave the way to a future in which people have more control over personal data, including rights of access and erasure, and portability, as well as enabling individuals to realize more of the value of data and at the same time gain trust in data sharing.

Since 2010, a European Data Protection Supervisor’s (EDPS) opinion on privacy in the digital age stated that “Privacy by Design” should be a key tool for ensuring citizens’ trust in ICTs [EDPS 2019] and “... *Such trust will only be secured if ICTs are reliable, secure, under individuals’ control and if the protection of their personal data and privacy is guaranteed*”.

The GDPR introduces a legal obligation to implement privacy design strategies in article 25. It imposes an obligation to adopt both technical and organizational measures. These measures must assure:

- automatic means for the collection of the informed data subject’s consent, and for the withdrawal of her given consent to the processing;

- the adoption of fair and appropriate measures to provide any information and communication to the data subject;
- the implementation of user interfaces for “privacy friendly” interactions with data subjects;
- the adoption of automatic means (or protocols) for the exercise of the data subject’s rights, in particular the right to erasure, the right to access, the right to be forgotten and data portability;
- the duty of the data controller is to “maintain a record of processing activities under its responsibility”;
- the adoption of security measures.

The above organizational measures must be supported by technical measures, which could include pseudonymization and data minimization, encryption, anonymization, aggregation, limitation of third party access, data usage control, audit, data logging and a secure communication protocol.

It is important to stress that these measures shall be adopted by design and by default, covering all the phases from design to implementation of privacy related applications, also taking into account the “state of the art” by staying updated on technical advances in privacy technologies, standards, regulations and recommendations.

Privacy preserving tools and models are needed to liberate the potential of personal data, allowing citizens to own and take control of their data, and to open SCs to innovations in service provision in compliance with the new GDPR. Methods and tools must contribute to security and interoperability in data connections between the data provider and the data consumer, putting the data subject in the loop in order to ensure real user-centric data management and ownership. SC processes need solutions that can act as an intermediary and as a tool of communication between data subjects and data controller and processors, by providing functionalities for lawful data sharing processes that have the ability to grant and withdraw consent to third parties. “Consent” is the basis for authorizing a data provider to release data to a data consumer, and authorizes the data consumer to process that data by referring to a data usage policy. It is important to support the entire end-to-end process in personal data processing, from the definition of policies to personal data sharing among an ecosystem of data-driven services. To ensure automation and interoperability among all the parties involved, consent and policies must be semantically described by referring to shared vocabularies. This semantic harmonization allows a semantic description of usage policies to be attached to data and to travel with it, allowing usage policies to be managed in such a way that the data controller and data subject can easily determine, for any kind of processing, for which purposes it is permitted and what, if any, are the related restrictions and obligations.

All these tools and methods will act as an intermediary and as means of communication between data subjects and data controller/processors. Thus, it is also necessary to investigate how to assure secure and certified communication among all the parties, allowing affordable, secure and trusted micro-transactions. We need to assure that the platform and the data users (providers and consumers) agree on a data usage policy that will eventually be linked to consent from the data subject. This agreement could be implemented by attaching it to a common distributed ledger infrastructure, in order to ensure forensic notarization, so that none of the parties may make any change without informing the other.

## 9.9 Roadmap

### 9.9.1 Short-term plan until the end of the project

For the last period of the project, we will finalize the implementation and evaluate the results of the integration of eIDAS authentication, privacy-preserving Attribute-Based Credentials and DLTs for a trustworthy and privacy-respecting authentication and authorization framework.

For the last period of the project, the SC demonstrator will integrate a MISP platform accessed through an implemented reverse proxy. This access will be controlled by the SC infrastructure. The use of the reverse proxy will increase the effectiveness of defences among stakeholders that share their cyber-threat intelligence. The pilot will integrate a MISP instance that retrieves cyber-threat information from compromised situations. End-users from the pilot infrastructure will gather this information and send it to the MISP instance through the Proxy. The implemented Proxy applies privacy-preserving techniques, following the guidelines of a privacy policy. Finally, the CTI will share it among other MISP instances from the CS4E project.

We plan to execute a second round of assessments on (i) the individual Social Engineering awareness and (ii) the organizational cyber posture in Genoa municipality. After the first round, the municipality adopted some countermeasures that should contribute to a better result from the assessments.

For the last period of the project, we will evaluate the results of our integration of pp-IdM (based on zero-knowledge proofs) for the achievement of privacy by design in the authentication and authorization modules of SCs.

Despite the energy devoted to investigating the main challenges related to GENERAL\_D, future research activities will include standardization of the XACML GDPR Policy Profile, validation of the GENERAL\_D proposal through additional case studies, discussion and validation of the proposal with legal experts so as to confirm the compliance with the GDPR, releasing a reference architecture of GENERAL\_D, and providing the user-story templates suitable for other legal frameworks.

The CaPe solution will be evaluated more deeply, taking into account the improvement in privacy after its integration into smart city service provisioning dealing with personal data. Further improvement of CaPe and GENERAL\_D will be investigated

#### 9.9.1.1 Cyber response and resilience & Cyber fault/failure detection and prevention

We plan to execute a second round of security evaluation on the Porto demonstrator, integrating the honeypot feature introduced in WP3. This should improve the awareness of the vulnerability assessment on the demonstrator. From a prevention perspective, RATING will give CISO a detailed view of the cyber-risk posture of Genoa municipality. This paves the way for countermeasure actions needed when a critical risk is identified, significantly increasing the resilience to cyberattacks.

#### 9.9.1.2 End user trusted data management

For the last period of the project, to be confident about data protection and taking into account and respecting the confidence and security of the end user, we will analyse and test our implementations (focusing on user-

side tools for, e.g. requesting data) to enhance and refine the final converging system based on zero knowledge tokens and capability-based access control in SC environments.

PTASC and ARGUS will be re-evaluated to include new modules from the assets. In the PTASC we aim to allow users to block specific domains using a middleware implementation on a router. In the context of ARGUS, we will allow users to use searchable encryption techniques to store metadata locally.

The evolution of the CaPe component for transparency will be evaluated in the SC scenario for user-centric consent management, its integration with eIDAS and its related evolution. CaPe evaluation and related evolution will contribute to future versions of MIM plus<sup>491</sup> specifications.

### 9.9.1.3 Interoperability between legacy and new systems

PTASC will be tested on a set of raspberry pi to evaluate the capabilities of current implementations.

### 9.9.1.4 Logging and monitoring

The last period of the project in the SC scenario will be focused on auditing and accountability procedures for personal data management, in particular related to consent management supported by adoption of the CaPe solution.

## 9.9.2 Beyond the end of the project plan

### 9.9.2.1 Security 2025

- **Increase of the attack surface:** As reported by the World Economic Forum,<sup>492</sup> devices connected to the IoT network will be much more numerous than the world population. By 2025, the number of IoT devices is expected to exceed 40 billion, more than four times the world's population. That is an enormous increase in the attack surface for the IoT world that needs to be addressed from the standardization and certification perspective.
- **Auditing of SC infrastructures:** Exacerbated by the explosion in the number of devices, it is necessary to enable the auditability of SC infrastructures. This challenge is even more difficult when we consider that monitoring and traceability must be applied while respecting privacy precepts. While this interaction is tackled on this vertical, further research into enabling technologies (DLT, access control mechanisms) and their integration will be necessary for accomplishing the ideal targets.
- **High dynamicity of environments:** Another relevant topic which is especially present on SC scenarios is the high dynamicity of environments and, specifically, security aspects. Current security models and mechanisms are too static. Thus, research into mechanisms more suited to dynamic environments (e.g. AI detection systems for complex attacks, lack of security and even auto-improvement of security policies) will be necessary. To enable this kind of research, new

---

<sup>491</sup> <https://living-in.eu/group/7/commitments/mims-plus-version-4-final>

<sup>492</sup> <https://www.weforum.org/agenda/2021/03/ai-is-fusing-with-the-internet-of-things-to-create-new-technology-innovations/>

standards for models that allow high extensibility and are adapted to the new workflows will also be a must.

### 9.9.2.2 Security 2030

- **Microservices logic:** The vertical systems should be reviewed from the point of view of modules structured at least with microservices logic, both for the domain logic and for the management of security and profiling to the various functions of the vertical itself. It will be natural to think of a single data management system with related tracking from the point of view of both consent (access, use, specific purposes) to the data, and the security model adopted, which will be integrated into a single platform that is able to manage all the logic of security and data access for both the user and the operators.
- **Lack of guarantee of uniqueness of the user's ID:** Basically, the new access management system that involves the current SPID and eIDAS systems should be allowed to evolve into an OpenID system, which could potentially lead to a global system for accessing services and would remedy the current problem of security in accessing data linked to the eIDAS authentication system, given the lack of guarantee of uniqueness of the user's ID. In this case a data breach could occur due to the lack of exposure of one's own data.

### 9.9.3 Milestones

We expect to have reached the following milestones by the end of the project:

- **Trusted Digital Platform:** Improved and finalized enhanced authorization and authentication framework, including extra capabilities such as usage analytics.
- **Cyber threat intelligence and analysis platform:** Full integration of CTI sharing platform (based on MISP) with DLT and SC infrastructure.
- **Successfully deployed CaPe instance for Genova Use Case** about consent management.
- **Full integration of PTASC and Briareos in the scenario and development of the front-end of the marketplace.**

## 9.10 Summary

This chapter focuses on the security of the Smart Cities ecosystem. The first sub-sections depict the big picture with a particular view about (i) the assets which are at risk, (ii) the ways to compromise these assets (section 9.3) and, (iii) the specific attacker list (section 9.4).

The SWOT Analysis (in section 9.6.2) showed that cybersecurity research has the responsibility to lead the development in this area, due to the fragmentation of micro-services already available in the SC's infrastructure. This can be a real opportunity to disrupt the market with a clear and shared vision about the needs and solutions provided by EU partners. On the other hand, there is a threat that efforts may be directed to vertical services without considering cross-interactions.

The area of Smart Cities can clearly contribute to European Digital Sovereignty through (i) regulation (such as the GDPR), (ii) application at the local/city level, and (iii) achievement of sovereignty in individual areas

such as AI sovereignty and 5G sovereignty. Finally, the COVID-19 pandemic, has forced the physical cities and the Smart Cities environment into a new reality: physical movement was reduced, most daily activities moved to cyberspace, and the fear of the virus spread has extended its grip all over Europe. In this challenging environment, we need to be able to use SC data in order to reduce the virus spread and achieve effective monitoring while at the same time making sure that we avoid mass citizen surveillance.

The research challenges linked to this very heterogeneous scenario were showed in section 9.5 and are listed here:

- Challenge 1: Trusted Digital Platform
- Challenge 2: Cyber threat intelligence and analysis platform
- Challenge 3: Cyber competence and awareness program
- Challenge 4: Privacy by design
- Challenge 5: Cyber response and resilience
- Challenge 6: End user trusted data management
- Challenge 7: Interoperability between legacy and new systems
- Challenge 8: Cyber fault/failure detection and prevention
- Challenge 9: Logging and monitoring
- Challenge 10: Information security and operational security

Activities in the next year should focus on (i) trusted digital platforms, (ii) cyber threat intelligence and analysis, (iii) information security and operational security, (iv) privacy by design and end-user trusted data management, (v) cyber response and resilience & cyber fault/failure detection and prevention, (vi) interoperability between legacy and new systems, (vii) cyber competence and awareness, and (viii) logging and monitoring.

## 10 Progress since D4.4

### 10.1 Open Banking

Since the last report, the following progress has been made:

- (1) The 12-month roadmap was a mapping of the whole end-to-end Open Banking process, involving all stakeholders, with a view to exposing security and privacy gaps. As far as we are aware, this challenge has still not been addressed, for very much the same reasons as before: there is still a lack of an end-to-end view of Open Banking processes, which begs the question as to why nothing has happened during the last 18 months.

The main reasons are that:

- Different actors are very focused on their own narrow sphere, earnestly trying to:
  - make the APIs work better (API providers)
  - get the compliance right (banks)
  - develop new business models (FinTechs)
  - wade through mountains of new licensing applications (national authorities)

Consequently, there are very few who are stepping back and looking at the picture as a whole and how the components fit together. One body that is surely taking a more holistic view is the regulator, who is constantly trying to find where there may be deficiencies in the ecosystem, such as whether:

- the banks are moving fast enough
- there are technical issues
- there is a level playing field
- the incentives to the market are right

However, the regulator will not have the technical or security competence to identify the real end-to-end chain and key security issues.

- There is really no great commercial motivation to go through and map out the whole process chain. It could be argued that this represents an opportunity for academic/research-oriented organisations to address it. Most researchers either focus on new revenue models (business), technical certificates (IT), or on social outcomes based on social sciences such as inclusion, transparency, fairness, use in the developing world, etc. Identifying the complete chain in this multidimensional ecosystem is complex. As listed above, there are many stakeholders: regulators (who are a whole ecosystem in themselves), national competent authorities, banks, FinTechs, certificate providers, customers, service providers and more. Not everyone has the competence to draw up the complete chain, to show the flow of information and identify the weak links.

As mentioned previously, CyberSec4Europe has a strong constituency of academic and corporate partners and, although it did not make a good use-case for the second cycle of the T5.1 (the demonstrator use-case), there is scope before the end of the project to advance this topic by adopting a holistic research approach and involving associates and other external partners.

- (2) The issues being addressed in the demonstrator use-cases have made good progress since the last report:

- a. **CYTILIS** (Cyber Threat Intelligence and Information Sharing) is demonstrating cooperation between a number of cross-border MISP instances in sharing information about banking cybersecurity events
- b. **OBSDIAN** (Open Banking Sensitive Data Sharing Network for Europe) is moving from the first phase cross-border proof-of-technology demo to experimentation between four French banks, using real data (in real time) with a more advanced set of sophisticated metrics. This further experimentation comes about as a result of sustained activity within the FBF's (French Banking Federation) fraud working group, which has generated widespread interest within the French banking community on what is possible—and not possible—within a centralised architecture facilitating information sharing about fraud.
- c. **Privacy-Preserving Verifiable Credentials**, using the VCUCIM asset, are now available on mobile devices and will be shown demonstrating secure eKYC for onboarding a new customer to a bank
- d. **OBACHT** (Open Banking API Architecture) provides an extension of what was demonstrated in the first phase using OAuth 2.0 with Poste Italiane. Given that Open Banking does not define many aspects of the OAuth implementation, this new analysis will demonstrate how banks can use the model as a framework and a starting point to develop their architecture and/or evaluate how to integrate the services provided by additional stakeholders.

## 10.2 Supply Chain Security Assurance

During the period since the definition of the second roadmap (D4.4 [Markatos 2021]) and the current roadmap, we have focused on the research and development of two assets: i) Blockchain platform and consensus algorithm, and ii) Workflow compliance assurance and accountability, under the umbrella of the Supply Chain platform demonstrator. These tasks were defined in the 12-month plan and 2-year plan of D4.4, related to the *integration of distributed workflows*, the *trusted exchange of information*, and the *integration of blockchain-based solutions*. The results obtained provide original solutions to several of the research goals that were highlighted in the supply chain challenges (cf. sections 4.6.11-4.6.14). More specifically, the advances in these assets related to the supply chain challenges are as follows:

- Regarding “Challenge 2, Security hardening of supply chain infrastructures, including cyber and physical systems” (section 4.6.12), the blockchain platform and consensus algorithm provides a hardened blockchain solution where *only authorised stakeholders are able to receive and access private information*.
- Precisely, regarding “Challenge 3, Security and privacy of supply chain information assets and goods” (section 4.6.13), the management of private data within the blockchain solution *facilitates the creation of a secure and privacy-aware data sharing infrastructure*. Additionally, the second asset, which focused on distributed workflows, *can provide automatic analysis of such workflows, identifying exceptions and anomalies*.

As mentioned above, these assets have been integrated into the supply chain demonstrators developed as part of Task 5.2, which focus on a) dispute resolution for retail supply chains, and b) compliance and accountability in distributed manufacturing. These demonstrators, whose second iteration is almost finished,

will provide the means to handle disputes in cross-organizational supply chain processes, and managing complex collaborative workflows through decentralized means.

### 10.3 Privacy-preserving identity management

During this year, we have worked on the tasks defined in the 2-year plan of D4.4 [Markatos 2021] for the various challenges related to privacy-preserving identity management. One of the tasks carried out has been the improvement of the maturity of our distributed p-ABC system. This has resulted in the full inclusion of a range of proofs for integers and dates, as well as some general implementation improvements, such as extra functionality for better efficiency in the underlying group computations. Related to this, we have also continued our work on the distributed oblivious identity management system as a whole, consolidating the implementation, including the new functionalities of the scheme. In addition, we have integrated the solution with W3C's Verifiable Credential specification, with ideas about modelling that can be applied to p-ABCs in general, and a first working implementation where the specification is used for serialization of the p-ABCs used [GTBS 2021]. Apart from that, we have worked on the blockchain deployment, achieving a mature deployment based on Hyperledger Ledger with Smart Contract support. This deployment enabled the integration and improvement of the distributed oblivious system and the adoption of the W3C Verifiable Credential, acting as a verifiable data registry and regulating the publication of critical data (public keys, schemas and even services and policies offered by dependent parties) through smart contracts. Further, the development of an issuer-hiding attribute-based credential scheme has been completed.

For the work mentioned in the 2-year plan of D4.4 [Markatos 2021], the work on researching the impact of GDPR and eIDAS on identity management has already produced partial results relating to GDPR interoperability and cross-border compliance. While the study was not specifically aimed at identity management, it contains relevant information on the implementation of identity management across the EU, including the age of consent, erasure of data and use of biometric data for purposes of identification. The results were published on the CyberSec4Europe website: <https://cybersec4europe.eu/heterogeneity-of-data-protection-legislation-in-the-eu/>. Full results will be published in D3.18.

Following the delivery of D4.4, the development of the passwordless authentication application has been completed and it has already been tested in a demo scenario in D3.13 [Resende 2021]. Furthermore, additional research has been performed into the security of passwordless authentication solutions, focusing on FIDO protocols [APX 2021] [GPX 2021].

### 10.4 Incident Reporting

During the period since the definition of the second roadmap (D4.4 [Markatos 2021]) and the current roadmap, the prototype of the Incident Reporting platform demonstrator has been extended and improved in the following features:

Regarding Challenges 1 and 2:

- The current version of the demonstrator supports a configurable number of incident reporting iterations depending on the configuration done by each regulation. In this way, once a first report is generated, it is possible to continue with a new data enrichment phase to produce an interim and/or a final report with additional information.

- The demonstrator has been extended to support the generation of reports following these regulatory frameworks: ECB/SSM, PSD2, TARGET2, NIS and eIDAS.
- The demonstrator includes the possibility of defining timers associated with the different regulations to trigger a notification escalation procedure. This procedure allows the platform to automatically send an email to the responsible person in case there is a delay in the generation and submission of the reports, adapted to the different regulatory framework specifications.
- The demonstrator has been extended to support the tracking of the security event lifecycle to register the main actions taken during the incident reporting workflow for each incident reported.

Regarding the Challenge 3:

- We have now identified the information registered in the Incident Reporting platform that the financial institutions will be willing to share with other stakeholders or entities through a threat intelligence platform.
- The demonstrator has been connected to a MISP instance to enable the capability of threat intelligence data sharing.

Additionally, the current roadmap includes the impacts of this demonstrator on climate change and democracy, and the contributions to the EU CyberSecurity Strategy for the Digital Decade. Furthermore, an analysis has been made of the major incidents in this vertical in the last 20 years and the problems in the incident reporting in the financial sector vertical that we would like to see solved in the next 10 years.

## 10.5 Maritime Transport

With respect to the expected goals addressed in the vertical's previous iteration of the research and development roadmap, CyberSec4Europe D4.4 "Research and Development Roadmap 2", January 2021 [Markatos 2021], within the past 12 months we have produced corresponding amendments and achievements which are described below.

As regards "Challenge 1: Early identification and assessment of risks, threats and attack paths for critical maritime systems", cyber-attack path discovery algorithms have been enhanced with machine learning techniques to capture more accurately the interdependencies within maritime transport systems and to perform more precisely the mapping of attack paths with threat agents. Preliminary results have been published in [GBS+2021]. Extended work on attack path discovery and analysis in a situational-aware manner, in terms of supporting adaptive risk assessment, is currently under process.

In relation to "Challenge 2: Security hardening of maritime infrastructures, including cyber and physical systems", security controls related to software hardening have been integrated into the MITIGATE platform and accompanying tools have been set up respectively. Furthermore, the examination of new controllers to improve its capacity and resolve possible bugs or malfunctions is an ongoing task.

Concerning "Challenge 4: System communication security", a demonstrator of a maritime trust infrastructure which considers the environmental limitations of the maritime transport sector (i.e. network availability and communication costs) has been set up and validated.

Finally, an initial prototype of the maritime transport security demonstrator has been set up as a result of works carried out within Task 5.5 of the project. Initial validation results have been reported in

CyberSec4Europe D5.3 “Validation of Demonstration Case Phase 1” [SB+2021] and published in [GPK+2021].

## 10.6 Medical Data Exchange

Since the previous iteration of the research and development roadmap (D4.4 [Markatos 2021]), the Medical Data Exchange demonstrator has updated and completed the following aspects.

Regarding the security, trust and privacy tools included in sections 8.8.1, 8.8.2, and 8.8.3:

- Implementation of the eIDAS connector for integrating the eIDAS network with the COVID-19 Data Exchange platform, through the French eIDAS node.
- Implementation of the FE2MED (crypto asset) providing end-to-end encryption mechanism between the data providers and the data consumers.

Regarding the regulation challenge included in section 8.8.4, the envisaged plan provided in document D4.4 [Markatos 2021] is confirmed:

- “In order to produce the GDPR guidelines the regulation, best practices and opinions provided by the European Commission and different supervisory authorities will be reviewed to create a comprehensive guideline, usable for as many situations and circumstance as possible.
- Additionally, research on Regulation matters and related tools will seek out ways for easier and better compliance with regulations such as GDPR and eIDAS.
- An analysis of interoperability and cross-border compliance of the eIDAS compliant electronic identification, security, and authentication services will be performed to identify flaws and compatibility of solutions between member states.” [Markatos 2021]

Related to the user experience challenge (section 8.8.5):

- Improvement of visualization and assessment tools in the COVID-19 Data Exchange platform and the design of user interface of DANS (anonymisation tool) asset.

Additionally, the impacts of this demonstrator on climate change and democracy, and the contributions to the EU CyberSecurity Strategy for the Digital Decade has been provided. Moreover, some updates on SWOT analysis have been done due to the impact of COVID-19 pandemic. Finally, a forecast for the future 10 years of the Medical Data Exchange demonstrator roadmap is included.

## 10.7 Smart Cities

**MURCIA:** During last year, we evolved the privacy-preserving authentication and authorization framework by adding proofs of range predicates, and we completed the integration of the zero-knowledge predicates with the XACML policy management system. In addition, we developed the implementation of

anonymization and generalization components and integrated them with an MISP instance for collection and privacy-preserving sharing of cyber-threat information. A new use-case was defined to share Cyber Threat Intelligence (CTI) among different parties in a privacy-preserving manner. In this use-case, cyber-attack evidence collected in the smart city of “MiMurcia” is exchanged across the platform for further use and analysis. This sharing is done through a Threat Information Platform called MISP that relates to other instances. However, these platforms lack privacy tools to protect the information. A proxy to these platforms was implemented; thus, the information is protected before it is exchanged. This proxy implements several Privacy Enhanced Technologies (PET) to protect the information by anonymizing it. In this way, it is obfuscated, avoiding a possible privacy leakage. Additionally, it implements CP-ABE to protect access to this information. With this cryptographic technique, only the receiver can access the information if they accomplish the privacy policies. To add trustworthiness to the platform and ensure the integrity of the data, the proxy leverages a blockchain to store partial information, or information that can be checked afterwards to prove provenance and integrity.

**GENOA:** During the last year, we executed the first round of assessment of cyber risk in the municipality organization, as well as carrying out a social-driven vulnerability assessment with interesting insights described in WP5 deliverables. These have paved the way for an improvement of the cybersecurity assets of the municipality. In the context of the CaPe solution, the following activities have been performed: 1. Update of requirements and use-case scenario; and 2. Specifications of CaPe integration with the IT system of the Municipality of Genova, in particular in relation to the integration with SPID, the Italian eIDAS scheme and plugin extension for consent collection.

**PORTO:** During the last year, we developed a system to integrate PTASC, an end-to-end identity provider for the IoT, and ARGUS cloud-of-clouds solutions to persistently store data generated in IoT adapted for the Fiware ecosystem. This helped the development of a laboratory prototype with similar features to the real development, but focused on the geolocation services. At the same time, we started the integration to construct the marketplace with the required changes to the Fiware architecture. In this process, we also enhance the security properties of the IoT sensors available throughout the city, using a Host Intrusion Detection System (HIDS), in this case briareos from WP3, and study the integration with a Honeypot module for enriching the security of the smart city. This motivated two publications in relevant journals from PTASC and ARGUS [RMB+ 2021], [SMR+ 2021].

## 11 Related Work

### 11.1 Concordia Roadmap (D4.4)

Concordia recently published a preliminary version of D4.4 “Cybersecurity Roadmap for Europe by CONCORDIA”.<sup>493</sup> The document presents a roadmap in cybersecurity along several different dimensions:

- Research and Innovation
- Education and Skills
- Economics and Investments
- Legal and Policy
- Certification and Standardization
- Community Building

#### 11.1.1 Threat Landscape

In the threat landscape, CONCORDIA made the following research-related recommendations:

- R1 Focus on persistent threats
- R2 Find a good trade-off between security level and domain peculiarities
- R3 Tailored security investments
- R4 Protection from insider threats
- R5 Consider the deployment environment untrusted
- R6 Digital twins and possible safety impact
- R7 Protect the user profiling capabilities
- R8 Protect the AI models, engines, and data pipelines from manipulations
- R9 Consider the networking peculiarities while designing system security
- R10 Protect from wide-band network-based localized DDoS
- R11 Protect edge computing nodes and services
- R12 Adoption of serverless computing
- R13 Protect against AI weaponized threats
- R14 Protection against deepfake
- R15 Conscious use of Social Networks
- R16 Deep understanding of layered architecture security
- R17 Sharing and multi-tenancy concerns
- R18 Consider the Virtualization/Containment weakness
- R19 Control misconfiguration issues and foster transparency
- R20 Avoid shadow IT
- R21 Monitoring of human errors
- R22 Continuous awareness campaign and training

---

<sup>493</sup> [https://www.concordia-h2020.eu/wp-content/uploads/2021/10/CONCORDIA\\_Roadmap.pdf](https://www.concordia-h2020.eu/wp-content/uploads/2021/10/CONCORDIA_Roadmap.pdf)

- R23 Protect the CIA triad of data
- R24 Protect from mobile and IoT malware
- R25 Adopt security-aware development pipelines
- R26 Consider the complexity of the deployment environment
- R27 Consider the miniaturization of the services
- R28 Protect CPS devices

The recommendations aim to protect devices, networks, systems, data and applications.

### **11.1.2 Research and Innovation**

In the area of research and innovation CONCORDIA proposed to focus on “Fighting Disinformation” and “Data Lakes” in the short term, on “Responsible Internet” in the midterm and on “Quantum Technologies” in the long term (see Figure 5 of D4.4 of Concordia).

### **11.1.3 Education and Skills**

The education and skills roadmap is organized in the short, medium and long term as follows:

#### **11.1.3.1 Short term**

- The design of a European Skills Framework for Cybersecurity
- Agreeing on the common Terminology linked to Education for cybersecurity professionals
- Mapping existing courses for professionals by structuring the information based on the Skills framework and applying the Terminology
- Guidelines for course co-design and co-development with the target industry.
- Develop courses targeting non-traditional industries
- The design of a Cybersecurity Skills Certification Framework that will incorporate the best practices of International Standards
- Define Cybersecurity Skills Certification Scheme
- Design a self-assessment tool for cybersecurity skills
- Building the Cybersecurity Skills readiness Radar
- Increase Opportunities for Women in Cyber

#### **11.1.3.2 Mid-Term**

- European Label for Courses for professionals
- Cybersecurity Skills for company insurance policy

#### **11.1.3.3 Long-Term Aims**

- Develop the Cybersecurity culture
- English as connecting language for online cybersecurity courses

### **11.1.4 Other Roadmaps**

The deliverable also presents roadmaps for Economics (chapter 6), for Investment (chapter 7), for legal and policy (chapter 8), for standardization and certification (chapter 9), and for community building (chapter

10). However, the closest (to our work) CONCORDIA roadmaps are the one for research and (to some extent) the one for education and skills.

## 11.2 Cyberwatching.eu EU Cybersecurity & Privacy Final Roadmap (D4.7)

This final version of the Cybersecurity and Privacy Roadmap (July 2021) summarises and shares the key points of the significant deliverables from within the cyberwatching.eu project, especially those that are relevant for the roadmap. Hence, this deliverable represents the culmination of the work of cyberwatching.eu and, according to the authors, could be used as a building block for further efforts after the end of the project which finished on 31 July 2021.

In addition, the document highlights a number of pre-existing roadmaps, including their conclusions and recommendations, from the EU, each of the pilot projects, ENISA, ECSO, JRC and NIST from the US. The benefit of this approach is to understand the commonalities and the differences in approach. The document also contains a selection of information relating to legislation, programmes and a summary of aspects of work done by cyberwatching.eu.

As this document (i.e. D4.5), covers the “pre-existing roadmaps”, there is no need to duplicate content by reporting on what is covered in the cyberwatching.eu deliverable.

Hence, in summary the roadmap from cyberwatching.eu shows the following key areas emerging:

- Data protection and privacy
- Cybersecurity and privacy by design
- Training / Education / Awareness
- Standardization and privacy
- International dialogue
- Building trust – establishment of an EU certification scheme
- Emerging Technologies

Unlike the CyberSec4Europe roadmap, cyberwatching.eu is primarily a long list of policy and research-oriented recommendations, derived from earlier deliverables and broken down into the areas listed above. Desired completion dates, strategic priorities and target audiences are not specified.

At the end of the document, the report provides its summation of the common areas and threads found across all the roadmaps and other material reviewed.

1. **Trust and Accountability** addressing the issue of confidence in which products, solutions and service that you use
2. **Governance** with respect to harmonisation, compliance, national application of regulations issues
3. **Data Security and Privacy** as this relates to the General Data Protection Regulation, while at the same time there is an urgent need for tools and guidance on compliance aspects
4. **Education, Training and Awareness** involving all of the specialised skillset to increase capabilities, capacity and expertise in cybersecurity, certification and especially standards, also with the goal of addressing the significant challenge of retaining expertise in Europe

5. **European and International Cyber Security Certification**, filling the gaps and striving to keep up with the evolution and expansion of emerging technologies
6. **Cross-border business requirements**, which were highlighted as a specific issue and challenge during the COVID pandemic
7. **SMEs** lack the resources and support tools and require training, as well as their issue of retaining trained Human Resources
8. **Cybersecurity standards** have issues related to cost, the understanding of experts in the field and new standards within the context of new and changing technologies
9. **Resilience** represents an important issue for critical infrastructure, as well as the economic and social fabric of society
10. The lack of an **Ethics Code of Conduct** as a result of changing, new and emerging technologies

As noted above, this is a fairly high level wish-list, or set of statements of intent, that would be difficult to translate into a workable research roadmap.

### 11.3 ECHO INTER-SECTOR CYBERSECURITY TECHNOLOGY ROADMAP (D4.3)

The ECHO project (European network of Cybersecurity centres and competence Hub for innovation and Operations) is one of 4 Pilot projects, launched by the European Commission, to establish and operate a Cybersecurity Competence Network (CCN). ECHO provides an approach for strengthening the proactive cyber defence of the European Union, through effective/efficient multi-sector collaboration.

ECHO includes 9 Work Packages (WP) from which WP4 is focused on the development of cybersecurity technology roadmaps as a result of the analysis related to current and emerging cybersecurity challenges and associated technologies. These roadmaps are expected to act as the foundations for new industrial capabilities and assist in the development of innovative technologies that will aim to address these cybersecurity challenges.

Overall, ECHO project includes the delivery of 6 cybersecurity technology roadmaps including:

- ECHO Early Warning System (E-EWS) delivered as part of the project
- ECHO Federated Cyber Range (E-FCR) delivered as part of the project
- At least 2 additional technology innovations to be completed as part of the project
- At least 2 additional technology innovations to be addressed by the future CCN

Due to the number of potential development opportunities, these roadmaps have been divided into sub-sections according to major technological areas described, called EPICs. For example, the EPICs for E-FCR include:

- **User experience** domain deals with how users of the Cyber Ranges and E-FCR interact with the tools
- **Connectivity** domain explores effect of future connectivity development
- **Scalability** discusses ways to scale the E-FCR platform
- **Platform** domain deals with Cyber Ranges platforms and integration of new tools
- **Exploitation** domain focuses on novel uses of the E-FCR platform

Those EPICs are further divided into sub-topics called User Stories (US), each describing specific technology drivers and their targets, technology alternatives and their timelines. For example, for E-EWS and E-FCR roadmaps, total of 29 user stories were identified and developed, some of them including multiple development opportunities for the ECHO platforms.

Apart from technical aspects, these roadmaps bring net legal and privacy issues that need to be addressed in order to create sustainable operation and provision of services in essentially global marketplace.

## 11.4 ENISA CYBERSECURITY RESEARCH DIRECTIONS FOR THE EU'S DIGITAL STRATEGIC AUTONOMY

In April 2021, ENISA published a report for the *Cybersecurity Research Directions for the EU's Digital Strategic Autonomy*. The report mainly focuses on the definition of EU's digital strategic autonomy and digital sovereignty, namely *the ability of Europe to source products and services, without undue influence from the outside world*, presenting the key areas for developing a digital strategic autonomy, and the societal factors that should be considered. According to a recent report of ENISA<sup>494</sup>, the European digital sovereignty includes three categories:

1. Data sovereignty over the EU citizens' personal data,
2. Digital sovereignty of the data-driven European industry,
3. Digital sovereignty of the EU and EU Member States

While a recent strategic note of the European Political Strategy Centre (EPSC) defines 3 dimensions:

1. The Industrial dimension that demands the ability of Europe to fulfil its digital needs by supporting the operational capability of Europe to leverage digital technologies, operate its critical infrastructure and to ensure their robustness to cyberattacks. The ability to control the critical digital infrastructure enables political strategic autonomy, namely Europe is able to make informed decisions freely and independently.
2. The Operational dimension is related to the resilience of the EU's communication infrastructures along with its ICT systems. A vulnerability in one service of one Member State can have major consequences for others and eventually Europe as a whole.
3. The Political dimension is related with digital sovereignty. The former Vice-President of the European Commission Viviane Reding, based on the more general definition of sovereignty (i.e., "the capacity to determine one's actions and norms")<sup>495</sup>, defined digital sovereignty as the "capacity to influence norms and standards of information technology"<sup>496</sup>.

The main scope of this report is to identify and analyse the key knowledge areas for developing products and services that cover the EU's needs and guarantee a resilient ICT infrastructure. Thus, in order for the

<sup>494</sup> ENISA, *Consultation paper – EU ICT industrial policy: Breaking the cycle of failure*, 2019 (<https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/eu-ict-industry-consultation-paper>).

<sup>495</sup> In 2016, Germany and France promoted European digital sovereignty – ANSSI, 'The European digital sovereignty – A common objective for France and Germany', April 2016 (<https://www.ssi.gouv.fr/en/actualite/the-european-digital-sovereignty-a-common-objective-for-france-and-germany/>).

<sup>496</sup> Reding, V., 'Digital sovereignty: Europe at a crossroads' (<https://institute.eib.org/wp-content/uploads/2016/01/Digital-Sovereignty-Europe-at-a-Crossroads.pdf>).

reader to comprehend the presented notions a number of fictional practical examples are presented to highlight the need for digital strategic autonomy in Europe as well as what will happen if Europe fails to maintain its digital strategic autonomy. Particularly, the report elaborates on 11 scenarios:

1. Interference with navigation services.
2. Untrusted AI
3. Disruption in the medical care system
4. No safety at home
5. Lack of supply chain availability
6. Absence of control over communication infrastructure
7. Need for post-quantum secure communications
8. Lack of control over a product or system lifecycle
9. Critical infrastructure interruptions
10. Loss of algorithmic control leading to loss of understanding of decision support algorithms
11. Lack of data

Furthermore, 7 key knowledge areas have been identified to cover the aforementioned scenarios. These knowledge areas are described below:

- **Data Security.** The majority of people did not know how much information they provide to an application, when they provided it, and for what reason this information is being used. On the other hand, top cloud providers are based outside Europe (e.g., Microsoft, Google, etc.), hence there are regulation (e.g., Cloud Act) that may force providers to grant access to EU citizens' data going against the provisions and regulations, such as GDPR. Towards this direction, EU has supported research project related to data protection, developed regulatory frameworks, as well as it has published numerous studies and reports. Finally, to maintain and further enhance its data-based digital economy, Europe should control key technologies from the following domains:
  - Understanding and mitigating vulnerabilities of AI
  - Ensuring the availability of machine learning and big data platforms that are sourced, hosted and sustainable in Europe
  - Developing new technologies for data security and privacy, to support advances in regulations and the emerging needs of the digital society.
  - Explainable AI
  - Securing decision support and actuating
  - Social trustworthiness of AI
- **Trustworthy Software Platforms.** With the heavily adoption of software in every day needs and in critical infrastructures, the development and establishment of trustworthy software platforms inside Europe is critical. Thus, specific actions should take place, including:
  - Trustworthy operating systems
  - Trustworthy middleware
  - Detection of malware and botnets
  - System and virtualisation security
  - Secure software development platforms
  - Risk assessment platforms
  - Trustworthy sensors
  - Open-cloud software services
- **Cyber Threat Management and Response.** The field of threat management and incident report is not new; however, ensuring the cyber threat management and response is a complex task. Europe needs to be able to design, develop, deploy, and preserve its own detection solutions to be able to

defend its critical infrastructures. The specific actions that should be considered include the following:

- Cyber threat intelligence
  - Cybersecurity analytics
  - Situational awareness
  - Attack detection, mitigation, and response
  - Deception
  - Cyber defence
  - Post-design and post-perimeter defence and response strategies
  - Thrusted information sharing
- **Trustworthy Hardware Platforms.** The fact that suppliers and manufactures of hardware platforms are mostly located outside Europe widens the threat scenarios. In the near future, autonomous cars/ships/buses, drones, IoT devices, 5G networks, etc. will be heavily used creating the need for Europe to source its own trustworthy hardware not only to secure its supply chain, but also to be able to control secure infrastructures of the future. Several actions can be performed to enhance the security of hardware including:
    - Bootstrap security
    - Hardware-induced vulnerabilities
    - Side channel attacks
    - Hardware-anchored cybersecurity tools
    - Open hardware architecture
    - Safe sensing
  - **Cryptography.** Cryptographic algorithms are one of the main pillars of cybersecurity. Although cryptography is increasingly being used in IT systems, its use in industrial controls, which are often part of critical infrastructures, is limited. With the increase of computing power, memory, and the progress of mathematical tools, it is clear that cryptographic algorithms and protocols are weakened. Hence, the research and standardization activities in cryptography should continue to assure the efficacy of available tools when confront emerging computing paradigms. Future actions should include:
    - Post-quantum cryptography
    - Basic cryptographic building blocks
    - Standards-based maintenance of cryptographic suites
    - Cryptographic protocols
    - Tools to support security validation of cryptographic implementations
    - Strong EU certification authority
  - **User-centric Security Practices and Tools.** A well-known issue of cybersecurity is that the weakest link of every organization is its employees. Thus, adversaries trying to gain access by exploiting human weaknesses (i.e., social engineering). Furthermore, cybersecurity solutions are a burden to standard IT users, which tend to believe that such solutions will reduce the productivity. Many actions need to be taken to convert cybersecurity solutions from a burden to an asset that helps the system function better including:
    - Privacy-enhancing technologies (PET)
    - Usable security
    - Human-centred security and privacy
    - Security visibility
    - Social engineering and human errors in cybersecurity

- Verifiable computing
- **Digital Communication Security.** Nowadays, the overall networking environment is moving from ownership-based infrastructure towards on-demand, pay-per-use networking and computing. Moving towards the era of virtual communication environments, Europe should maintain trust and efficiency in communication services, since it is essential for the development of a digital Europe. The specific actions that Europe should perform are:
  - Network services as critical infrastructure
  - Network security
  - IoT security
  - Virtual networks

The report states that social dimensions are a key part of the EU's digital strategic autonomy and sovereignty, since it cannot be achieved without a skilled workforce and a regulatory and legal framework. Therefore, from the workforce perspective, the report mentions that efforts should be expended on bringing students closer to cybersecurity curricula, on skill development actions (e.g., certificates), as well as on ethic and legal dimensions. From the regulatory and legal perspective, it is mentioned that the development of tools for evaluating GDPR compliance, along with the evaluation of cybersecurity certification schemes is critical.

## 11.5 ENISA THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS

The Treat Landscape for Supply Chain Attacks report elaborates on supply chain attacks providing a thorough description of their traits that discriminates them from other cyberattacks. The report identifies 4 key elements that a supply chain attack contains:

- **Supplier:** the entity that supplies a product or service to another entity.
- **Supplier Assets:** valuable elements used by the supplier to produce the product or service.
- **Customer:** the entity that consumes the product or service produced by the supplier.
- **Customer Assets:** valuable elements owned by the target.

A supply chain attack is defined as “*a combination of at least two attacks*”, where the first attack targets the supplier to gain access to its assets, which are later used to attack the customer (i.e., For an attack to be classified as a supply chain attack both the supplier and the customer have to be targets). A taxonomy for supply chain attacks has been proposed that aims to facilitate the community understanding the various parts of supply chain attacks, comparing them with other cyberattacks, as well as identifying incidents as supply chain attacks. The taxonomy categorizes the attacks based on 4 types:

1. Attack Techniques Used to Compromise the Supply Chain (e.g., Malware infection, social engineering, brute-force, open-source intelligence, etc.)
2. Supplier Assets Targeted by the Supply Chain Attack (e.g., code, configurations, data, software libraries, processes, hardware, people, etc.)
3. Attack Techniques Used to Compromise the Customer (e.g., trusted relationship, drive-by compromise, phishing, etc.)
4. Customer Assets Targeted by the Supply Chain Attack (e.g., data, intellectual property, software, processes, bandwidth, etc.)

Later, the well-known attack techniques that used to compromise supply chains attacks analyzed in this report including:

- Malware infection
- Social engineering
- Brute-force attack
- Exploiting software vulnerability
- Exploiting configuration vulnerability
- Physical attack or modification
- Open-source intelligence (OSINIT)
- Counterfeiting

Following, the lifecycle of supply chain attacks is discussed in order to further understand their functionality and help organizations develop robust defence mechanisms. Particularly, the lifecycle of a supply chain attack is composed by two main parts, the attack on the supplier (i.e., supplier APT attack) and the attack on the customer (i.e., customer APT attack). Each of these attacks is often complex, requiring one attack vector, one plan of action, and careful execution. Also, these attacks may take months to be successful and may go undetected for a long time. Moreover, prominent supply chain attacks from January 2020 to July 2021 are presented along with a classification based on the proposed taxonomy. The selected attacks contain the attacks performed on *Solarwinds*, *Mimecast*, *Ledger*, *Kaseya*, and *Sita*. The report also provides a thorough analysis of several supply chain incidents based on various factors, such as the timeline, the flow of attacks, the attackers' goal, and the attack vectors. Finally, the authors conclude with several recommendations and best practices regarding the protection against supply chain attacks and the development of resilient supply chain environments.

## 11.6 ENISA Threat Landscape 2021

In the 2021 edition of the ENISA Threat Landscape (ETL) report, an annual report on the status of the cybersecurity threat landscape that identifies prime threats, major trends have been observed with respect to threats, threat actors, and attack techniques. The report also described relevant mitigation measures. The time span of the ETL 2021 report was April 2020 to July 2021 and was referred to as the "reporting period" throughout the report. During the reporting period, the prime threats identified include:

- Ransomware
- Malware
- Cryptojacking
- E-mail related threats
- Threats against data
- Threats against availability and integrity
- Disinformation – misinformation
- Non-malicious threats
- Supply-chain attacks

In the ETL report the first 8 cybersecurity threat categories were discussed. For each of the identified threats, attack techniques, notable incidents and trends were discussed, along with proposed mitigation measures. Regarding trends, during the reporting period, the ETL reported:

- Ransomware has been assessed as the prime threat for 2020-2021.
- Governmental organisations have stepped up their game at both national and international level.
- Cybercriminals were increasingly motivated by monetisation of their activities, e.g. ransomware.
- Cryptocurrency remained the most common payout method for threat actors.
- A malware decline was observed in 2020 and continued during 2021. In 2021, there was an increase in threat actors resorting to relatively new or uncommon programming languages to port their code.
- The volume of cryptojacking infections attained a record high in the first quarter of 2021, compared to recent years. The financial gain associated with cryptojacking incentivised threat actors to carry out these attacks.
- COVID-19 was still the dominant lure in campaigns for e-mail attacks.
- There was a surge in healthcare sector related data breaches.
- Traditional DDoS (Distributed Denial of Service) campaigns in 2021 were more targeted, more persistent, and increasingly multivector. The IoT (Internet of Things) in conjunction with mobile networks resulted in a new wave of DDoS attacks.
- A spike in non-malicious incidents was observed, as the COVID-19 pandemic became a multiplier for human errors and system misconfigurations, up to the point that most of the breaches in 2020 were caused by errors.

Understanding the trends related to threat actors, their motivations and their targets greatly assists in planning cybersecurity defences and mitigation strategies. This was an integral part of the overall threat assessment, since it allows security controls to be prioritised and a dedicated strategy to be devised, based on the potential impact and likelihood of threat materialisation. For the purposes of ETL 2021, the following four categories of cybersecurity threat actors were considered:

- State-sponsored actors
- Cybercrime actors
- Hacker-for-hire actors
- Hacktivists

Through continuous analysis, ENISA derived trends and points of interest for each of the major threats presented in ETL 2021. The key findings and judgments in this assessment were based on multiple and publicly available resources that were provided in the references used for the development of the document. The report was mainly targeted at strategic decision-makers and policymakers, but also the technical cybersecurity community.

The ENISA Threat Landscape (ETL) report provided a general overview of the cybersecurity threat landscape. The ETL report was partly strategic and partly technical, with information relevant to both technical and non-technical readers. This year's work has been supported by a newly formatted ENISA *ad hoc* Working Group on Cybersecurity Threat Landscapes (CTL).

Cybersecurity attacks have continued to increase through the years 2020 and 2021, not only in terms of vectors and numbers but also in terms of their impact. The COVID-19 pandemic had an impact on the cybersecurity threat landscape. One of the more enduring developments that resulted from the COVID-19 pandemic was a lasting shift to a hybrid office model. Therefore, cybersecurity threats related to the pandemic and exploiting the “new normal” were becoming mainstream. This trend increased the attack

surface and, as a result, a rise was noticed in the number of cyber-attacks targeting organisations and companies through home offices.

In general, cybersecurity threats were on the rise. Spurred by an ever-growing online presence, the transitioning of traditional infrastructures to online and cloud-based solutions, advanced interconnectivity, and the exploitation of new features of emerging technologies such as Artificial Intelligence (AI), the cybersecurity landscape has grown in terms of sophistication of attacks, their complexity, and their impact. Notably, the threat to supply chains and their significance, due to their potentially catastrophic cascading effects, reached the highest position among major threats, so much so that ENISA produced a dedicated threat landscape for this category of threat. It is worth noting that in this iteration of the ETL, particular focus was given on the impact of cyber threats in various sectors, including the ones listed in the NISD. Interesting insights were drawn from the particularities of each sector when it came to the threat landscape, as well as potential interdependencies and areas of significance. Accordingly, sectorial threat landscapes merit further attention.

There have also been some notable steps from the side of defenders in the cyber community this year, as well as the policy makers. The global community begun to realise the importance of communication and cooperation in examining and tracking cybercriminals, with ransomware (the most prominent threat for the reporting period of ETL 2021) becoming a prime item in agendas for meetings on strategy among global leaders.

This year, ENISA took a step back and consolidated threat categories in a move towards integration and better representation of similar threats. This was part of ongoing efforts towards a revamped threat taxonomy and will help in establishing trends methodologically over the next few years.

The ETL 2021 was based on a variety of open-source information and cyber threat intelligence sources. It identified major threats, trends and findings, and provided relevant high-level mitigation strategies.

### **11.6.1 Most Important Threats**

A series of cyber threats emerged and materialised in the course of 2020 and 2021. Based on the analysis presented in ETL 2021, ENISA identified and focused on the following important threat groups, which were highlighted because of their prominence during the reporting period, their popularity, and the impact that materialisation of these threats had.

#### **11.6.1.1 Ransomware**

Malware is software or firmware intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity, or availability of a system. The threat of malware has consistently ranked high for many years, albeit at a decreasing rate during the reporting period of ETL 2021. The use of new attack techniques and some major wins for the law enforcement community impacted the operations of relevant threat actors.

#### **11.6.1.2 Malware**

Malware is software or firmware intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity, or availability of a system. The threat of malware has consistently ranked high for many years, albeit at a decreasing rate during the reporting period of ETL 2021. The use of

new attack techniques and some major wins for the law enforcement community impacted the operations of relevant threat actors.

### **11.6.1.3 Cryptojacking**

Cryptojacking, or hidden cryptomining, is a type of cybercrime where a criminal secretly uses a victim's computing power to generate cryptocurrency. With the proliferation of cryptocurrencies and their ever-increasing uptake by the wider public, an increase in corresponding cybersecurity incidents was observed.

### **11.6.1.4 E-mail related threats**

E-mail related attacks are a bundle of threats that exploit weaknesses in the human psyche and in everyday habits, rather than technical vulnerabilities in information systems. Interestingly and despite the many awareness and education campaigns against these types of attacks, the threat persisted to a notable degree. In particular, the compromise of business e-mails and advanced sophisticated techniques for extracting monetary gains were on the rise.

### **11.6.1.5 Threats against data**

This category encompasses data breaches/leaks. A data breach or data leak is the release of sensitive, confidential, or protected data to an untrusted environment. Data breaches can occur because of a cyber-attack, an insider job, unintentional loss, or exposure of data. The threat continued to be high, since access to data was a prime target for attackers for numerous reasons, e.g. extortion, ransom, defamation, and misinformation.

### **11.6.1.6 Threats against availability and integrity**

Availability and integrity are the target of a plethora of threats and attacks, among which the families of Denial of Service (DoS) and Web Attacks stand out. Strictly related to web-based attacks, DDoS is one of the most critical threats to IT systems, targeting their availability by exhausting resources, causing decreases in performance, loss of data, and service outages. The threat was consistently ranked high in the ENISA Threat Landscape, because of both its manifestation in actual incidents and its potential for high impact.

### **11.6.1.7 Disinformation – misinformation**

Disinformation and misinformation campaigns were on the rise, spurred by the increased use of social media platforms and online media, as well because of the increase of people's online presence due to the COVID-19 pandemic. This group of threats made its first appearance in the ETL; however, its importance in the cyber world was high. Disinformation and misinformation campaigns were frequently used in hybrid attacks to reduce the overall perception of trust, a major proponent of cybersecurity.

### **11.6.1.8 Non-malicious threats**

Threats are commonly considered as voluntary and malicious activities carried out by adversaries that have some incentives to attack a specific target. With this category, the threats where malicious intent is not apparent are covered. These are mostly based on human errors and system misconfigurations, but they can also refer to physical disasters that target IT infrastructures. Also attributed to their nature, these threats have a constant presence in the annual threat landscape and are a major concern for risk assessments.

## 11.6.2 Key Trends

The list below summarises the main trends observed in the cyber threat landscape during the reporting period. These were also reviewed in detail throughout the various chapters comprising the ENISA Threat Landscape of 2021.

- Highly sophisticated and impactful supply chain compromises proliferated, as highlighted by the dedicated ENISA Threat Landscape on Supply Chains. Managed service providers were high-value targets for cybercriminals.
- COVID-19 drove cyber espionage tasking and created opportunities for cybercriminals.
- Governmental organisations stepped up their game at both national and international level. Increased efforts were observed from governments to disrupt and take legal action against state-sponsored threat actors.
- Cybercriminals were increasingly motivated by monetisation of their activities, e.g. ransomware. Cryptocurrency remained the most common payout method for threat actors.
- Cybercrime attacks increasingly targeted and impacted critical infrastructure.
- Compromise through phishing e-mails, and brute-forcing on Remote Desktop Services (RDP) remained the two most common ransomware infection vectors.
- The focus on Ransomware as a Service (RaaS) type business models increased over 2021, making proper attribution of individual threat actors difficult.
- The occurrence of triple extortion ransomware schemes increased strongly over the course of 2021. The malware decline that was observed in 2020 continued during 2021. In 2021, an increase in threat actors resorting to relatively new or uncommon programming languages to port their code was observed.
- Malware targeting container environments became much more prevalent, with novel evolutions like file-less malware being executed from memory.
- Malware developers kept finding ways to make reverse engineering and dynamic analysis harder.
- The volume of cryptojacking infections attained a record high in the first quarter of 2021, compared to the last few years. The financial gain associated with cryptojacking incentivised the threat actors to carry out these attacks.
- The volume of cryptomining in 2021 and cryptojacking activities were at a record high.
- A shift from browser to file-based cryptojacking was observed.
- COVID-19 was still the dominant lure in campaigns for e-mail attacks.
- Business E-mail Compromise (BEC) increased, grew in sophistication, and became more targeted.
- The Phishing-as-a-Service (PhaaS) business model was gaining prevalence.
- Threat actors shifted their attention towards vaccine information in the context of threats to data and information.
- There was a surge in healthcare sector related data breaches.
- Traditional DDoS (Distributed Denial of Service) attacks were moving towards mobile networks and the IoT (Internet of Things).
- Ransom Denial of Service (RDoS) was the new frontier of Denial of Service attacks.

- Sharing of resources in virtualised environments acted as an amplifier of DDoS attacks.
- DDoS campaigns in 2021 became more targeted and much more persistent and increasingly multivector.
- Artificial intelligence (AI)-enabled disinformation supported attackers in carrying out their attacks.
- Phishing was at the heart of disinformation attacks and strongly exploits people's beliefs.
- Misinformation and disinformation were at the core of cybercrime activities and were increasing at an unprecedented rate.
- The disinformation-as-a-Service (DaaS) business model grew significantly, spurred by the increasing impact of the COVID-19 pandemic and the need to have more information.
- In 2020 and 2021, a spike in non-malicious incidents was observed, as the COVID-19 pandemic became a multiplier for human errors and system misconfigurations, up to the point that most of the breaches in 2020 were caused by errors.
- There was a spike in cloud security non-malicious incidents.

## 11.7 EU Security Union Strategy (COM(2020) 605 final)

“COM(2020) 605 on the EU Security Union Strategy”<sup>497</sup> is a communication of the European Commission to the European Parliament, the European Council, The European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy. The document provides an analysis of new global threats and challenges to the European society and identifies four interdependent strategic priorities and actions to be taken forward at the EU level, in full respect of fundamental rights.

**A future-proof security environment** focused on critical infrastructure protection and resilience, cybersecurity, and protecting public spaces. The identified key actions are: Legislation on the protection and resilience of critical infrastructure; Revision of the Network Information Systems Directive; An initiative on the operational resilience of the financial sector; Protection and cybersecurity of critical energy infrastructure and network code on cybersecurity for cross-border electricity flows; A European Cybersecurity Strategy; Next steps towards the creation of a Joint Cyber Unit; Common rules on information security and cybersecurity for EU institutions, bodies and Agencies; Stepped up cooperation for the protection of public spaces, including places of worship; and Sharing of best practices on addressing misuse of drones.

**Tackling evolving threats** focusing on cybercrime, modern law enforcement, countering illegal content online, and hybrid threats. The identified key actions are: Ensuring that the cybercrime legislation is implemented and fit for purpose; a Strategy for a more effective fight against child sexual abuse; proposals on the detection and removal of child sexual abuse material; an EU approach on Countering Hybrid Threats; review of the EU operational protocol for countering hybrid threats (EU Playbook); and assessment of how to enhance law enforcement capacity in digital investigations.

---

<sup>497</sup> <https://ec.europa.eu/info/sites/default/files/communication-eu-security-union-strategy.pdf>

**Protecting Europeans from terrorism and organised crime** focusing also on radicalization. The identified key actions are: a counter-terrorism agenda for the EU, including renewed anti-radicalisation actions in the EU; new cooperation with key third countries and international organisations against terrorism; an agenda on tackling organised crime, including trafficking in human beings; an EU Agenda on Drugs and Action Plan 2021-2025; Assessment of the European Monitoring Centre for Drugs and Drug Addiction; 2020-2025 EU Action Plan on Firearms trafficking; Review of legislation on freezing and confiscation and on Asset Recovery Offices; An assessment of the Environmental Crime Directive; An EU Action Plan against Migrant Smuggling, 2021-2025.

**A strong European security ecosystem** focusing on cooperation and information exchange, the contribution of strong external borders, strengthening security research and innovation, skills and awareness raising. The identified key actions are: Strengthening of Europol mandate; Exploring an EU “Police Cooperation Code” and police coordination in times of crisis; Strengthening Eurojust to link judicial and law enforcement authorities; Revision of the Advance Passenger Information Directive; Communication on the external dimension of Passenger Name Records; Strengthening cooperation between the EU and Interpol; A framework to negotiate with key third countries on sharing of information; Better security standards for travel documents; Exploring a European Innovation hub for internal security.

## 11.8 EU CyberSecurity Strategy for the Digital Decade (JOIN(2020) 18 final)

“JOIN(2020) 18 on the EU’s Cybersecurity Strategy for the Digital Decade”<sup>498</sup> is a joint communication of the European Commission and the European Parliament on the EU’s Cybersecurity Strategy for the Digital Decade. The document identifies a set of strategic initiatives within four main areas:

**Resilience, technological sovereignty and leadership:** Adoption of revised NIS Directive; Regulatory measures for an Internet of Secure Things; Through the CCCN investment in cybersecurity (notably through the Digital Europe Programme, Horizon Europe and recovery facility) to reach up to €4.5 billion in public and private investments over 2021-2027; An EU network of AI-enabled Security Operation Centres and an ultra-secure communication infrastructure harnessing quantum technologies; Widespread adoption of cybersecurity technologies through dedicated support to SMEs under the Digital Innovation Hubs; Development of an EU DNS resolver service as a safe and open alternative for EU citizens, businesses and public administration to access the Internet; and Completion of the implementation of the 5G Toolbox by the second quarter of 2021.

**Building operational capacity to prevent, deter and respond:** Complete the European cybersecurity crisis management framework and determine the process, milestones and timeline for establishing the Joint Cyber Unit; Continue implementation of cybercrime agenda under the Security Union Strategy; Encourage and facilitate the establishment of a Member States’ cyber intelligence working group residing within the EU INTCEN; Advance the EU’s cyber deterrence posture to prevent, discourage, deter and respond to malicious cyber activities; Review the Cyber Defence Policy Framework; Facilitate the development of an EU

<sup>498</sup> <https://ec.europa.eu/info/sites/default/files/communication-eu-security-union-strategy.pdf>

“Military Vision and Strategy on Cyberspace as a Domain of Operations” for CSDP military missions and operations; Support synergies between civil, defence and space industries; and Reinforce cybersecurity of critical space infrastructures under the Space Programme.

**Advancing a global and open cyberspace:** Define a set of objectives in international standardisation processes, and promote these at international level; Advance international security and stability in cyberspace, notably through the proposal by the EU and its Member States for a Programme of Action to Advance Responsible State Behaviour in Cyberspace (PoA) in the United Nations; Offer practical guidance on the application of human rights and fundamental freedoms in cyberspace; Better protect children against child sexual abuse and exploitation, as well as a Strategy on the Rights of the Child; Strengthen and promote the Budapest Convention on Cybercrime, including through the work on the Second Additional Protocol to the Budapest Convention; Expand EU cyber dialogue with third countries, regional and international organisations, including through an informal EU Cyber Diplomacy Network; Reinforce the exchanges with the multi-stakeholder community, notably by regular and structured exchanges with the private sector, academia and civil society; and Propose an EU External Cyber Capacity Building Agenda and an EU Cyber Capacity Building Board.

**Cybersecurity in the EU institutions, bodies and agencies:** Regulation on Information Security in the EU institutions, bodies and agencies; Regulation on Common Cybersecurity Rules for EU institutions, bodies and agencies; A new legal base for CERT-EU to reinforce its mandate and funding.

## 11.9 EU Strategy to tackle Organised Crime 2021-2025 (SWD(2021) 74 final)

“COM(2021) 170 final on the EU Strategy to tackle Organised Crime 2021-2025”<sup>499</sup> is a communication of the European Commission to the European Parliament, the European Council, The European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy. The document identifies key actions to be taken against organized crime within four main areas:

### **Boosting law enforcement and judicial cooperation:**

- The Commission will: Propose strengthening the Prüm framework (Q4 2021); Propose the creation of an EU Police Cooperation Code (Q4 2021); Propose revision of the Advanced Passenger Information Directive (Q1 2022); Establish a collaboration platform for Joint Investigation Teams (Q4 2021); Work with all relevant stakeholders, to streamline, expand and modernise the European Multidisciplinary Platform Against Criminal Threats (EMPACT) and establish it as the EU flagship instrument to fight organised and serious international crime through a set of actions and a legislative proposal (2023); Significantly reinforce funding for EMPACT through the Internal Security Fund for the period 2021-2027; Start negotiations for agreements on cooperation between Eurojust and third countries; Step up negotiations on cooperation between Europol and third countries; Reinforce, jointly with the European External Action Service, international cooperation with third countries and international organisations.

---

<sup>499</sup> [https://ec.europa.eu/home-affairs/system/files/2021-04/14042021\\_eu\\_strategy\\_to\\_tackle\\_organised\\_crime\\_2021-2025\\_com-2021-170-1\\_en.pdf](https://ec.europa.eu/home-affairs/system/files/2021-04/14042021_eu_strategy_to_tackle_organised_crime_2021-2025_com-2021-170-1_en.pdf)

- The European Parliament and the Council are invited to: Advance in the legislative negotiations on the Revision of the Europol Regulation, including the amendments to the Schengen Information System Regulation, with the aim of reaching a swift agreement.
- The Council is invited to adopt the recommendation to open the negotiations with Interpol on an EU-Interpol cooperation agreement.

**Effective investigations:**

- The Commission will: Propose amendments to the Environmental Crime Directive (Q4 2021); Strengthen the provisions on enforcement against illegal shipments of waste as part of its proposal amending the waste shipment regulation (Q2 2021); Establish an EU Toolbox against counterfeiting, setting out principles for joint action, cooperation and data sharing among law enforcement authorities, right holders and intermediaries (2022); Propose an Action Plan on trafficking of cultural goods (2022); Explore the possibility for the Union to accede to the Council of Europe Medicrime;
- Member States are urged to: Join and strengthen the @ON Network on mafia type organised crime groups and explore a more structured integration of a targeted approach against criminal networks into EMPACT; Establish or further develop coordination structures at national level or specialised bodies in law enforcement and judiciary authorities focused on tackling organised crime structures; Accede and ratify the Council of Europe Medicrime Convention.
- Member States and Europol are urged to: Develop common identification criteria to select and investigate High Value Targets and prioritise investigations against individuals and criminal networks posing the highest security risk in the EU; Develop a strategic and tactical intelligence picture of high-risk organised crime groups; Reinforce strategic and operational cooperation in the fight against counterfeiting of medical products, including with the European Anti-Fraud Office and the European Union Intellectual Property Office and at global level.

**Eliminating profits generated by organised crime and preventing infiltration into the legal economy and society:**

- The Commission will: Propose the revision of the Confiscation Directive and the Council Decision on Asset Recovery Offices (2022); Assess existing EU anti-corruption rules (2022); Promote cooperation and the exchange of information on the link between corruption and organised crime, including through Europol.
- Member States are urged to: Systematically conduct financial checks while investigating organised crime and, as soon as the financial environment indicates the presence of criminal assets, systematically undertake asset recovery investigations; Swiftly transpose the Directive on facilitating access to financial information by the deadline of August 2021; Exchange strategic information with those sectors at risk of being infiltrated by organised criminality groups (public-private partnerships); Enhance the specialisation of law enforcement services, and strengthen the bodies responsible for investigations, prosecutions and judicial proceedings of high-level corruption cases.
- Member States and Europol are urged to: Improve the intelligence picture on the threat of infiltration in the legal economy, by assessing the risks and methods used by organised crime groups.

## **Making law enforcement and the judiciary fit for the digital age:**

- The Commission will: Analyse and outline possible approaches and solutions on data retention for law enforcement and judiciary and consult Member States on these by the end of June 2021; Propose a way forward to address lawful and targeted access by law enforcement authorities to encrypted information in the context of criminal investigations. This approach should be based on a thorough mapping of how member states deal with encryption and on a multi-stakeholder process to explore and assess the concrete lawful options; Encourage and facilitate full and swift Member State participation in the e-Evidence Digital Exchange System (e-EDES); Develop, through its Joint Research Centre, a monitoring tool to gather intelligence on illegal activities developing in the Darknet; Support the development of training modules and materials and support training delivery by CEPOL, EJTN and national training institutions;
- Europol is urged to: Coordinate a comprehensive analysis of technological gaps and needs in the domain of digital investigation; Create a repository for tools, allowing law enforcement to identify and access state-of-the-art solutions; Create and maintain a database of experts in investigations and forensics related to specialised areas such as the Internet of Things or cryptocurrencies.
- CEPOL is urged to: Create certification/accreditation schemes for digital investigation experts; Provide and regularly update a Training Competencies Framework, together with Europol.
- The European Parliament and Council are urged to: Urgently adopt the e-evidence proposals to ensure speedy and reliable access to e-evidence for authorities.

### **11.10 Europol IOCTA**

The Internet Organized Crime Threat Assessment (IOCTA) is an annual report of cybercrime delivered by Europol. A core finding of the report, in the 2021 edition, is the persistence of the pandemic related to COVID-19, which directly affects cybercrime. Specifically, the pandemic has, for a second year, driven and increased cybercrime activities, since (a) attackers exploit the fact that more people are potentially vulnerable when they work remotely from home (IT internal security policies are often relaxed), and (b) children, who are also potential targets, spent more time using the Internet.

The report enumerates specific findings along 5 different domains, which we briefly abbreviate here as (a) crime-as-a-service, (b) advances in ransomware, (c) child sexual abuse material (CSAM), (d) on-line fraud, and (e) dark web. We discuss the major findings for each topic below and we conclude with some recommendations.

#### **11.10.1 Crime-as-a-service**

Cybercrime has evolved through automated tools (access-as-a-service, malware-as-a-service) that give the opportunity for ordinary users to commit cybercrime. As part of the automation, technologies that are heavily used include (a) crypto-currencies (for money laundering), and (b) VPNs for encrypted communications. These automated tools can be purchased by anyone, and can be easily found using the dark web infrastructure. This automation has transformed the actual malicious actors; attackers are now end-users of cyber-criminal services. This can have further impact in defending cybercrime. Investigations for cybercrime related incidents do not affect the cybercrime ecosystem, since very often the malicious actors are just end users of offensive services.

### 11.10.2 Advances in ransomware

Ransomware is still a major cybercrime force. However, it has radically changed from targeting masses of users to very focused targets, such as private companies, healthcare and education sectors, critical infrastructures, and governmental institutions. This shift indicates that ransomware operators choose their targets based on their financial ability to comply with higher ransom demands and their need to be able to resume their operations instantly. Additionally, ransomware now has more sophisticated mechanics since the goal is to potentially disrupt an entire digital-supply chain, which is typically composed of several different architectures/platforms. Ransomware attacks are now realized by sophisticated engines/kits that include exploit payloads for a series of different vulnerabilities. Finally, *ransom* is no longer connected just with decrypting sensitive files, but is much more aggressive, since attackers threaten their victims with exfiltrating sensitive data to the public (e.g. to journalists using VoIP) or with DDoS attacks.

Mobile malware has increased in the form of banking trojans. This form of software is usually installed in Android devices and is capable in stealing user credentials, OTPs used in 2FA, or passwords associated with crypto wallets.

### 11.10.3 Child Sexual Abuse Material (CSAM)

CSAM has been significantly increased as a result of the pandemic. There has been a steep increase in online grooming activities on social media and online gaming platforms, while children spend more time on the Internet, especially during lockdowns. Moreover, children now join the Internet at a younger age. Finally, the production of self-generated material is a key threat. This material is displaying increasingly younger children. It is important to mention that more CSAM cases are recorded in the victim's environment, possibly under the directions of people in the victim's trusted circle.

One major implication in tracking CSAM is the ePrivacy directive of 2002, which aims at ensuring confidentiality of communications and personal data but *does not* contain legal exceptions related to the detection of CSAM. This can slow down the investigation and, on many occasions, the resolution of CSAM incidents.

### 11.10.4 On-line fraud

Increased on-line shopping due to COVID-19 leads to on-line scams and an increase in phishing attacks. Card-not-present fraud (i.e. stealing card numbers and utilizing them for purchases that do not require the card physically) is under control as travel restrictions curb ATM attacks. However, attackers still try to leverage the increase in on-line shopping by stealing and using credit card numbers.

### 11.10.5 Dark web

The dark web facilitates cybercrime and now very often offers malware-as-a-service. Although LEAs can frequently take down specific markets, offenders can quickly migrate to a new service. Dark Web users are increasingly using Wickr and Telegram as communication channels or to bypass market fees, and

anonymous cryptocurrencies, such as Monero, and swapping services. Grey infrastructure, which includes legitimate technologies (e.g. secure communication, anonymous communications, obfuscation) retargeted for offensive goals is increasingly helping Dark Web users thrive.

## Recommendations

- *Remove certain legal obstacles for investigators.* The privacy of individuals should be protected, but, on the other hand, must not interfere with official investigations for resolving cybercrime activities, such as CSAM incidents.
- *More officers, tools and training needed.* As the technology used by attackers evolves (e.g. use of cryptocurrencies, advanced obfuscation techniques, automated kits for exploitation), the defenders must be equally prepared through receiving the necessary training and tools.
- *A broader cooperative focus.* Cybercrime has no borders and can span different territories that do not have a common legislation framework, or even different entities within a given nation. International cooperation should be key, as well as cooperation at the national level (e.g. between economic crime and cybercrime).
- *Integrate law enforcement in the cybersecurity ecosystem.* It should be mandatory for major cyber incidents affecting critical sectors to be reported to LEAs, just as they are reported to CSIRTs when it comes to other root causes, without needing a victim report to bootstrap an official investigation.
- *Streamline information sharing and enhance awareness campaigns.* Companies not based in the EU can decide to reveal limited information upon an LEA investigation. The EU framework allows sharing of data under an LEA investigation: that is much more useful and therefore enforcing this policy outside EU should be helpful. Additionally, awareness of cybercrime should be raised at all ages (including children and parents) through carefully organized campaigns.

## 12 Summary

In the context of the CyberSec4Europe project, we publish a yearly research and development roadmap. Unlike other similar road mapping activities, which may aim to cover all (or most) aspects of cybersecurity, our roadmaps aim to explore emerging threats and to prioritise research directions, mainly in the areas of the **seven verticals** that have been identified in the project: (i) open banking, (ii) supply-chain security assurance, (iii) privacy-preserving identity management, (iv) incident reporting, (v) maritime transport, (vi) medical data exchange, and (vii) smart cities. Our second roadmap (Deliverable D4.4) was published in 2021 and focused on landscaping the research areas of the verticals and establishing the most important priorities [Markatos 2021].

This document, the third roadmap in the series, focused on

- (i) *updating* the research priorities,
- (ii) explaining how we interact with important dimensions and policies including
  - a. ***Climate Change***
  - b. the ***Public Health*** and COVID-19 challenge, and
  - c. the ***EU Cybersecurity Strategy for the Digital Decade***
- (iii) explaining how the chosen research priorities map into the future:
  - a. *Security 2025*, and
  - b. *Security 2030*

Some of the priorities identified and/or areas that need more attention include:

- **Open Banking:**
  - Mapping of stakeholder interaction in end-to-end Open Banking processing
  - Setting up and discontinuing business relationships
  - Cross-border cooperation under differing legislation and security controls
  - Convenient and Compliant Authentication
  - Real time Revocation of Right of Access
  - Corporate Open Banking Security
- **Supply chain security assurance:**
  - Detection and management of supply chain security risks
  - Security hardening of supply chain infrastructures, including cyber and physical systems
  - Security and privacy of supply chain information assets and goods
  - Management of the certification of supply partners
- **Privacy-Preserving Identity Management**
  - System-based credential hardening
  - Unlinkability and minimal disclosure
  - Distributed oblivious identity management
  - Privacy preservation in blockchain
  - Password-less authentication
  - GDPR and eIDAS impact on Identity Management
  - Identity Management Solutions for the IoT
- **Incident Reporting**
  - Lack of harmonization of procedures

- Facilitate the collection and reporting of incident and/or data leaks
- Promote a collaborative approach for sharing incident reports to increase risk quantification, mitigation and thus overall cyber resilience
- **Maritime Transport**
  - Early identification and assessment of risks, threats and attack paths for critical maritime systems
  - Security hardening of maritime infrastructures, including cyber and physical systems
  - Resilience of critical maritime systems
  - Maritime system communication security
  - Securing autonomous ships
- **Medical Data Exchange**
  - Mechanisms for preserving user data privacy
  - Trustworthiness on the data exchange platform
  - Accomplish regulation during the data sharing process
  - Data exchange platform user experience
- **Smart Cities**
  - Trusted Digital Platform
  - Cyber threat intelligence and analysis platform
  - Cyber competence and awareness program
  - Privacy by design
  - Cyber response and resilience
  - End user trusted data management
  - Interoperability between legacy and new systems
  - Cyber fault/failure detection and prevention
  - Logging and monitoring
  - Information security and operational security

## 13 References

- [AA 2004] S. Andersen and V. Abella. "Changes to Functionality in Microsoft Windows XP Service Pack 2, Part 3: Memory Protection Technologies." Data Execution Prevention. *Microsoft TechNet article*, 2004. Accessed November, 2021.
- [AAG+ 2019] Anisetti, Marco, Claudio A. Ardagna, Filippo Gaudenzi, and Ernesto Damiani. "A Continuous Certification Methodology for DevOps." In *Proceedings of the 11th International Conference on Management of Digital EcoSystems*, pp. 205-212. 2019.
- [AAK+ 2018] Anjum, Adeel, Tahir Ahmed, Abid Khan, Naveed Ahmad, Mansoor Ahmad, Muhammad Asif, Alavalapati Goutham Reddy, Tanzila Saba, and Nayma Farooq. "Privacy preserving data by conceptualizing smart cities using MIDR-Angelization." *Sustainable cities and society* 40 (2018): 326-334.
- [AAWA 2016] AAWA. AAWA project introduces the project's first commercial ship operators, 2016. Accessed November, 2021. <https://www.rolls-royce.com/media/press-releases/2016/pr-12-04-2016-aawa-project-introduces-projects-first-commercial-operators.aspx>
- [ABH+ 2020] Abbasi, Babak, Toktam Babaei, Zahra Hosseinifard, Kate Smith-Miles, and Maryam Dehghani. "Predicting solutions of large-scale optimization problems via machine learning: A case study in blood supply chain management." *Computers & Operations Research* 119 (2020): 104941.
- [ABE 2021] Abe, Y., Arisaka, K., Kaneda, K., and K. Iwamura. "A supply chain management system to prevent counterfeiting and trace different transactions instead of using PUF device." 18th International Conference on e-Business ICE-B 2021, SciTePress (2021): 101-108.
- [ABEL 2009] Abbasi, Babak, Toktam Babaei, Zahra Hosseinifard, Kate Smith-Miles, and Maryam Dehghani. "Predicting solutions of large-scale optimization problems via machine learning: A case study in blood supply chain management." *Computers & Operations Research* 119 (2020): 104941.
- [Abulamddi 2017] Abulamddi, M. F. "A Survey on techniques requirements for integrating safety and security engineering for cyber-physical systems." *J. Comput. Commun* 5 (2017): 94-100.
- [ABS 2018]. American Bureau of Shipping (ABS). "Cybersecurity implementation for the marine and offshore industries, In: ABS (Ed.), ABS CyberSafety" Vol.2.
- [AGK 2019] Amro, Ahmed, Vasileios Gkioulos, and Sokratis Katsikas. "Connect and protect: Requirements for maritime autonomous surface ship in urban passenger transportation." In *Computer security*, pp. 69-85. Springer, Cham, 2019.
- [AHM 2021] Ahmed Khan, I., Nour Moustafa, D., Pi, D., Hussain, Y., and N. A. Khan. "DFE-SC4N: A Deep Federated Defence Framework for Protecting Supply Chain 4.0 Networks." *IEEE Transactions on Industrial Informatics*, in press (2021).
- [AKM+ 2021] Abraham, Andreas, Karl Koch, Stefan More, Sebastian Ramacher, and Miha Stopar. "Privacy-Preserving eID Derivation to Self-Sovereign Identity Systems with Offline Revocation." In *The*

20th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2021). IEEE Computer Soc., 2021.

[AMY+ 2018] Allal, Abdelmoula Ait, Khalifa Mansouri, Mohamed Youssfi, and Mohammed Qbadou. "Reliable and cost-effective communication at high seas, for a safe operation of autonomous ship." In *2018 6th International Conference on Wireless Networks and Mobile Communications (WINCOM)*, pp. 1-8. IEEE, 2018.

[AKLT 2020] Amro, Ahmed, Georgios Kavallieratos, Konstantinos Louzis, and Christoph A. Thieme. "Impact of cyber risk on the safety of the MilliAmpere2 Autonomous Passenger Ship." In *IOP Conference Series: Materials Science and Engineering*, vol. 929, no. 1, p. 012018. IOP Publishing, 2020.

[Akritidis 2010] Akritidis, Periklis. "Cling: A Memory Allocator to Mitigate Dangling Pointers." In *USENIX security symposium*, pp. 177-192. 2010.

[ANSSI EBIOS 2020] ANSSI, Agence nationale de la sécurité des systèmes d'information. EBIOS Risk Manager - The method (EBIOS RM). Accessed November, 2021. <https://www.ssi.gouv.fr/guide/ebios-risk-manager-the-method/>

[AMM+ 2018] Agrawal, Shashank, Peihan Miao, Payman Mohassel, and Pratyay Mukherjee. "PASTA: password-based threshold authentication." In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 2042-2059. 2018.

[AMN+ 2020] Aslam, Mudassar, Bushra Mohsin, Abdul Nasir, and Shahid Raza. "FoNAC-An automated Fog Node Audit and Certification scheme." *Computers & Security* 93 (2020): 101759.

[AMY+ 2018] Allal, Abdelmoula Ait, Khalifa Mansouri, Mohamed Youssfi, and Mohammed Qbadou. "Reliable and cost-effective communication at high seas, for a safe operation of autonomous ship." In *2018 6th International Conference on Wireless Networks and Mobile Communications (WINCOM)*, pp. 1-8. IEEE, 2018.

[APX 2021] Angelogianni, Anna, Ilias Politis, and Christos Xenakis. "How many FIDO protocols are needed? Surveying the design, security and market perspectives." *arXiv preprint arXiv:2107.00577* (2021).

[ASA 2018] Abu, Md Sahrom, Siti Rahayu Selamat, Aswami Ariffin, and Robiah Yusof. "Cyber threat intelligence—issue and challenges." *Indonesian Journal of Electrical Engineering and Computer Science* 10, no. 1 (2018): 371-379.

[ASS+ 2018] Ahmadian, Amir Shayan, Daniel Strüber, Volker Riediger, and Jan Jürjens. "Supporting privacy impact assessment by model-based privacy analysis." In *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, pp. 1467-1474. 2018.

[AUTOSHIP 2019]. EU H2020 project "Autonomous Shipping Initiative for European Waters", 2019. Accessed November, 2021. <https://www.autoship-project.eu/>

[AWA+ 2020] Alqubaisi, Fatima, Ahmad Samer Wazan, Liza Ahmad, and David W. Chadwick. "Should We Rush to Implement Password-less Single Factor FIDO2 based Authentication?" In *2020 12th Annual Undergraduate Research Conference on Applied Computing (URC)*, pp. 1-6. IEEE, 2020.

[AWW 2017] Alberts, Christopher, John Haller, Charles Wallen, and Carol Woody. "Assessing DoD system acquisition supply chain risk management." *CrossTalk* 30, no. 3 (2017): 4-8.

[BADA 2021] Bada, A.O., Damianou, A., Angelopoulos, C.M., and V. Katos. "Towards a Green Blockchain: A Review of Consensus Mechanisms and their Energy Consumption" 17th International Conference on Distributed Computing in Sensor Systems DCOSS'21 (2021): 503-511.

[BBC 2019] Bernabe, Jorge Bernal, Jose Luis Canovas, Jose L. Hernandez-Ramos, Rafael Torres Moreno, and Antonio Skarmeta. "Privacy-preserving solutions for blockchain: Review and challenges." *IEEE Access* 7 (2019): 164908-164940.

[BCBMM 2021] M. Barbareschi, V. Casola, A. De Benedictis, E. L. Montagna and N. Mazzocca, "On the Adoption of Physically Unclonable Functions to Secure IIoT Devices," in *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7781-7790, Nov. 2021, doi: 10.1109/TII.2021.3059656.

[BCS 2021] Balusamy, Balamurugan, Naveen Chilamkurti, and Seifedine Kadry, eds. *Green Computing in Smart Cities: Simulation and Techniques*. Springer Nature, 2020. ISBN: 978-3-030-48141-4

[BCM 2019] Bartolini, Cesare, Antonello Calabró, and Eda Marchetti. "Enhancing Business Process Modelling with Data Protection Compliance: An Ontology-based Proposal." In *ICISSP*, pp. 421-428. 2019.

[BCS 2021] Balamurugan Balusamy, Naveen Chilamkurti, Seifedine Kadry, "Green Computing in Smart Cities: Simulation and Techniques", ISBN: 978-3-030-48141-4, Springer, 2021

[BCH+ 2015] Baldimtsi, Foteini, Jan Camenisch, Lucjan Hanzlik, Stephan Krenn, Anja Lehmann, and Gregory Neven. "Recovering lost device-bound credentials." In *International Conference on Applied Cryptography and Network Security*, pp. 307-327. Springer, Cham, 2015.

[BDH 2018] Basin, David, Søren Debois, and Thomas Hildebrandt. "On purpose and by necessity: compliance under the GDPR." In *International Conference on Financial Cryptography and Data Security*, pp. 20-37. Springer, Berlin, Heidelberg, 2018.

[BDL+ 2019] Bartolini, Cesare, Said Daoudagh, Gabriele Lenzini, and Eda Marchetti. "Towards a Lawful Authorized Access: A Preliminary GDPR-based Authorized Access." *ICSOF 2019* (2019): 331-338.

[BDVA 2020] López de Vallejo, I., Scerri, S., Tuikka, T. (eds) (2020) Towards a European-Governed Data Sharing Space. Brussels. Accessed November, 2021. [https://www.bdva.eu/sites/default/files/BDVA%20DataSharingSpaces%20PositionPaper%20V2\\_2020\\_Final.pdf](https://www.bdva.eu/sites/default/files/BDVA%20DataSharingSpaces%20PositionPaper%20V2_2020_Final.pdf)

[BDM+ 2020] Bernabe, Jorge Bernal, Martin David, Rafael Torres Moreno, Javier Presa Cordero, Sébastien Bahloul, and Antonio Skarmeta. "ARIES: Evaluation of a reliable and privacy-preserving European identity management framework." *Future Generation Computer Systems* 102 (2020): 409-425.

[BEK+ 2021] Jan Bobolz, Fabian Eidens, Stephan Krenn, Sebastian Ramacher, Kai Samelin. Issuer-Hiding Attribute-Based Credentials. CANS 2021.

[BEF 2019] Boneh, Dan, Saba Eskandarian, and Ben Fisch. "Post-quantum EPID signatures from symmetric primitives." In *Cryptographers' Track at the RSA Conference*, pp. 251-271. Springer, Cham, 2019.

[BFH+ 2020] Baum, Carsten, Tore Frederiksen, Julia Hesse, Anja Lehmann, and Avishay Yanai. "PESTO: proactively secure distributed single sign-on, or how to trust a hacked server." In *2020 IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 587-606. IEEE, 2020.

[BFP+ 2018] Becue, Adrien, Yannick Fourastier, Isabel Praça, Alexandre Savarit, Claude Baron, Baptiste Gradussofs, Etienne Pouille, and Carsten Thomas. "CyberFactory# 1—Securing the industry 4.0 with cyber-ranges and digital twins." In *2018 14th IEEE International Workshop on Factory Communication Systems (WFCS)*, pp. 1-4. IEEE, 2018.

[BHB 2019] Ben-Daya, Mohamed, Elkafi Hassini, and Zied Bahroun. "Internet of things and supply chain management: a literature review." *International Journal of Production Research* 57, no. 15-16 (2019): 4719-4742.

[BGS 2015] Brown, Sarah, Joep Gommers, and Oscar Serrano. "From cyber security information sharing to threat management." In *Proceedings of the 2nd ACM workshop on information sharing and collaborative security*, pp. 43-49. 2015.

[BHH 2013] Balfanz, Dirk, Brad Hill, and Jeff Hodges. "Fido uaf protocol specification v1. 0." (2013).

[BHR 2017] Bernabé, Jorge Bernal, José Luis Hernández Ramos, and Antonio Fernandez Gómez-Skarmeta. "Holistic privacy-preserving identity management system for the internet of things." *Mob. Inf. Syst.* 2017 (2017): 6384186-1.

[BIMCO 2021A] Baltic and International Maritime Council. (BIMCO), "The guidelines on cyber security onboard ships." Version 4.0., 2021.

[BIMCO 2021B] BIMCO, Cyber Security Workbook for On Board Ship Use, 2021, 2nd Edition.

[Bizjak 2019] Bizjak, Tony. "Sacramento, Calif., Transit System Recovers from Ransomware Attack," 22 November 2017. Accessed November, 2021. <https://www.govtech.com/security/Sacramento-Calif-Transit-System-Recovers-from-Ransomware-Attack.html>

[BLC 2020] Berbecaru, Diana Gratiela, Antonio Lioy, and Cesare Cameroni. "Providing Login and Wi-Fi Access Services With the eIDAS Network: A Practical Approach." *IEEE Access* 8 (2020): 126186-126200.

[BLW 2017] Batalden, Bjorn-Morten, Per Leikanger, and Peter Wide. "Towards autonomous maritime operations." In *2017 IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA)*, pp. 1-6. IEEE, 2017.

- [BLZ+ 2020] Bouras, Mohammed Amine, Qinghua Lu, Fan Zhang, Yueliang Wan, Tao Zhang, and Huansheng Ning. "Distributed ledger technology for eHealth identity privacy: state of the art and future perspective." *Sensors* 20, no. 2 (2020): 483.
- [BMF+ 2018] Bieker, Felix, Nicholas Martin, Michael Friedewald, and Marit Hansen. "Data protection impact assessment." *Privacy and Identity Management* 526 (2018): 207-220.
- [BMM 1992] Bellovin, Steven Michael, and Michael Merritt. "Encrypted key exchange: Password-based protocols secure against dictionary attacks." (1992).
- [BN 2014] Backes, Michael, and Stefan Nürnberg. "Oxymoron: Making fine-grained memory randomization practical by allowing code sharing." In *23rd {USENIX} Security Symposium ({USENIX} Security 14)*, pp. 433-447. 2014.
- [BMZ 2018] Bach, L. M., Mihaljevic, B., & Zagar, M. (2018, May). Comparative analysis of blockchain consensus algorithms. In *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 1545-1550). IEEE.
- [BNM+ 2014] Bonneau, Joseph, Arvind Narayanan, Andrew Miller, Jeremy Clark, Joshua A. Kroll, and Edward W. Felten. "Mixcoin: Anonymity for bitcoin with accountable mixes." In *International Conference on Financial Cryptography and Data Security*, pp. 486-504. Springer, Berlin, Heidelberg, 2014.
- [BO 2020] Bouchelaghem, Siham, and Mawloud Omar. "Secure and efficient pseudonymization for privacy-preserving vehicular communications in smart cities." *Computers & Electrical Engineering* 82 (2020): 106557.
- [Boyson 2014] Boyson, Sandor. "Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems." *Technovation* 34, no. 7 (2014): 342-353.
- [BPR 2000] Bellare, Mihir, David Pointcheval, and Phillip Rogaway. "Authenticated key exchange secure against dictionary attacks." In *International conference on the theory and applications of cryptographic techniques*, pp. 139-155. Springer, Berlin, Heidelberg, 2000.
- [BSW 2007] Bethencourt, John, Amit Sahai, and Brent Waters. "Ciphertext-policy attribute-based encryption." In *2007 IEEE symposium on security and privacy (SP'07)*, pp. 321-334. IEEE, 2007.
- [BSW 2011] Boneh, Dan, Amit Sahai, and Brent Waters. "Functional encryption: Definitions and challenges." In *Theory of Cryptography Conference*, pp. 253-273. Springer, Berlin, Heidelberg, 2011.
- [BTB+ 2020] Bolbot, Victor, Gerasimos Theotokatos, Evangelos Boulougouris, and Dracos Vassalos. "A novel cyber-risk assessment method for ship systems." *Safety Science* 131 (2020): 104908.
- [Bund 2016] Jakob Bund, "Cybersecurity and democracy: Hacking, leaking, and voting." European Union Institute for Security Studies (EUISS), 2016.
- [BVH+ 2019] Bartolomeu, Paulo C., Emanuel Vieira, Seyed M. Hosseini, and Joaquim Ferreira. "Self-sovereign identity: Use-cases, technologies, and challenges for industrial iot." In *2019 24th IEEE*

*International Conference on Emerging Technologies and Factory Automation (ETFA)*, pp. 1173-1180. IEEE, 2019.

[BW 2009] Beggs, Christopher, and Matthew Warren. "Safeguarding Australia from cyber-terrorism: a proposed cyber-terrorism SCADA risk framework for industry adoption." (2009).

[BWC 2010] Berkeley, Alfred R., Mike Wallace, and Constellation COO. "A framework for establishing critical infrastructure resilience goals." *Final Report and Recommendations by the Council, National Infrastructure Advisory Council* (2010): 18-21.

[BZ 2006] Berger, Emery D., and Benjamin G. Zorn. "DieHard: Probabilistic memory safety for unsafe languages." *Acm sigplan notices* 41, no. 6 (2006): 158-168.

[BZA 2021] Bano, Muneera, Didar Zowghi, and Chetan Arora. "Requirements, politics, or individualism: What drives the success of covid-19 contact-tracing apps?." *Ieee Software* 38, no. 1 (2020): 7-12.

[CAL+ 2016] Cárdenas, Alvaro A., Saurabh Amin, Zong-Syun Lin, Yu-Lun Huang, Chi-Yen Huang, and Shankar Sastry. "Attacks against process control systems: risk assessment, detection, and response." In *Proceedings of the 6th ACM symposium on information, computer and communications security*, pp. 355-366. 2011.

[Casey 2007] Casey, Timothy. "Threat agent library helps identify information security risks." Intel White Paper 2 (2007).

[Cavoukian 2019] Cavoukian, Ann. "Privacy by design: The 7 foundational principles." *Information and privacy commissioner of Ontario, Canada* 5 (2009): 12.

[CBB 2016] Cherdantseva, Yulia, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, and Kristan Stoddart. "A review of cyber security risk assessment methods for SCADA systems." *Computers & security* 56 (2016): 1-27.

[CC 2018] Meharipedia. Avada. MEHARI standard (2018). Developed and updated since 1996 by Clusif and Clusiq (2018). Accessed November, 2021. <http://meharipedia.x10host.com/wp/telechargements/document2/>

[CDL 2020] Camenisch, Jan, Manu Drijvers, Anja Lehmann, Gregory Neven, and Patrick Towa. "Short threshold dynamic group signatures." *IACR Cryptol. ePrint Arch. 2020* (2020): 16.

[CDM 2019] Calabrò, Antonello, Said Daoudagh, and Eda Marchetti. "Integrating access control and business process for GDPR compliance: A preliminary study." In *ITASEC*. 2019.

[CDV 2013] Cheminod, Manuel, Luca Durante, and Adriano Valenzano. "Review of security issues in industrial networks." *IEEE transactions on industrial informatics* 9, no. 1 (2012): 277-293.

[CER 2019] Cerrudo, Cesar. "An emerging US (and world) threat: Cities wide open to cyber attacks." *Securing Smart Cities* 17 (2015): 137-151.

[Chaum 1981] Chaum, David L. "Untraceable electronic mail, return addresses, and digital pseudonyms." *Communications of the ACM* 24, no. 2 (1981): 84-90.

- [Chaum 1983] Chaum, David. "Blind signatures for untraceable payments." In *Advances in cryptology*, pp. 199-203. Springer, Boston, MA, 1983.
- [Chaum 1985] Chaum, David. "Security without identification: Transaction systems to make big brother obsolete." *Communications of the ACM* 28, no. 10 (1985): 1030-1044.
- [CKY+ 2021] Chang, Chia-Hsun, Christos Kontovas, Qing Yu, and Zaili Yang. "Risk assessment of the operations of maritime autonomous surface ships." *Reliability Engineering & System Safety* 207 (2021): 107324.
- [CL 2001] Camenisch, Jan, and Anna Lysyanskaya. "An efficient system for non-transferable anonymous credentials with optional anonymity revocation." In *International conference on the theory and applications of cryptographic techniques*, pp. 93-118. Springer, Berlin, Heidelberg, 2001.
- [CL 2002] Camenisch, Jan, and Anna Lysyanskaya. "A signature scheme with efficient protocols." In *International Conference on Security in Communication Networks*, pp. 268-289. Springer, Berlin, Heidelberg, 2002.
- [CL 2004] Camenisch, Jan, and Anna Lysyanskaya. "Signature schemes and anonymous credentials from bilinear maps." In *Annual international cryptology conference*, pp. 56-72. Springer, Berlin, Heidelberg, 2004.
- [Clang10] Clang 10 - Control Flow Integrity. Accessed November, 2021. <https://clang.llvm.org/docs/ControlFlowIntegrity.html>
- [CMB+ 2011] Cimpean, Dan, Johan Meire, Vincent Bouckaert, Stijn Vande Castele, Aurore Pelle, and Luc Hellebooge. "Analysis of cyber security aspects in the maritime sector." (2011). Accessed November, 2021. [https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1/at\\_download/fullReport](https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1/at_download/fullReport)
- [CMS 2010] Jan Camenisch, Sebastian Modersheim, & Dieter Sommer. "A formal model of identity mixer". In: *International Workshop on Formal Methods for Industrial Critical Systems*. Springer Heidelberg, 2010, pp. 198–214.
- [CMJ 2015] Campbell, Brian, Chuck Mortimore, and M. Jones. "Security assertion markup language (SAML) 2.0 profile for OAuth 2.0 client authentication and authorization grants." *Internet Engineering Task Force (IETF)* (2015).
- [CNIL 2021] French Commission Nationale de l'Informatique et des Libertés. "The open source PIA software helps to carry out data protection impact assessment." Accessed November, 2021. <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment>
- [COC 2021] Cocco, L., Tonelli, R., and M. Marchesi. "Blockchain and Self Sovereign Identity to Support Quality in the Food Supply Chain." *Future Internet*, vol. 13, no. 12 (2021): 301.

[COMPACT 2018] COMPACT Project, "Overall COMPACT architecture," (H2020 Project, G.A.740712), 2018.

[CO 2011] Cabinet Office. "Keeping the country running: natural hazards and infrastructure." *Improving the UK's ability to absorb, respond to and recover from emergencies* (2011).

[CPM+ 1998] Cowan, Crispan, Calton Pu, Dave Maier, Jonathan Walpole, Peat Bakke, Steve Beattie, Aaron Grier, Perry Wagle, Qian Zhang, and Heather Hinton. "Stackguard: automatic adaptive detection and prevention of buffer-overflow attacks." In *USENIX security symposium*, vol. 98, pp. 63-78. 1998.

[CRF+ 2018] Chhetri, Sujit Rokka, Sina Faezi, Nafiul Rashid, and Mohammad Abdullah Al Faruque. "Manufacturing supply chain and product lifecycle security in the era of industry 4.0." *Journal of Hardware and Systems Security* 2, no. 1 (2018): 51-68.

[CRS 1998] Clemens, P. L., and Rodney J. Simmons. "System safety and risk management: NIOSH instructional module." *US Department of Health and Human Services* (1998).

[CS 2017] Cui, Jin, and Giedre Sabaliauskaite. "On the alignment of safety and security for autonomous vehicles." *Proc. IARIA CYBER* (2017): 1-6.

[CS 2018] Cui, Jin, and Giedre Sabaliauskaite. "US \$\$^ \$\$: An Unified Safety and Security Analysis Method for Autonomous Vehicles." In *Future of Information and Communication Conference*, pp. 600-611. Springer, Cham, 2018.

[CSH+ 2014] Charlebois, Sylvain, Brian Sterling, Sanaz Haratifar, and Sandi Kyaw Naing. "Comparison of global food traceability regulations and requirements." *Comprehensive reviews in food science and food safety* 13, no. 5 (2014): 1104-1123.

[CSP+ 2020] Cha, Jeonghun, Sushil Kumar Singh, Yi Pan, and Jong Hyuk Park. "Blockchain-Based Cyber Threat Intelligence System Architecture for Sustainable Computing." *Sustainability* 12, no. 16 (2020): 6401.

[CSKP 2021] Cha, Jeonghun, Sushil Kumar Singh, Tae Woo Kim, and Jong Hyuk Park. "Blockchain-empowered cloud architecture based on secret sharing for smart city." *Journal of Information Security and Applications* 57 (2021): 102686.

[CSS, 1999] Custer, Rodney L., Joseph A. Scarella, and Bob R. Stewart. "The modified Delphi technique-A rotational modification." (1999).

[CySiMS] Cyber Security in Merchant Shipping. Accessed November, 2021. <http://cysims.no/>

[CZ 2019] Conners, James S., and Daniel Zappala. "Let's authenticate: Automated cryptographic authentication for the web with simple account recovery." *Who Are You* (2019).

[Daffey 2018] Daffey, Kevin, "Technology Progression of Maritime Autonomous Surface Ships", In the context of IMO "MSC 100: One hundred sessions enhancing safety and security of international shipping", Rolls-Royce plc. December 2018. Accessed November, 2021. [https://wwwcdn.imo.org/localresources/en/MediaCentre/IMOMediaAccreditation/Documents/MSC%20100%20special%20session%20presentations/20181203\\_Technology\\_Progression\\_In\\_MASS\\_IMO\\_Final\\_For\\_PDF.pdf](https://wwwcdn.imo.org/localresources/en/MediaCentre/IMOMediaAccreditation/Documents/MSC%20100%20special%20session%20presentations/20181203_Technology_Progression_In_MASS_IMO_Final_For_PDF.pdf)

- [DAV 2021] Davies J., and Y. Wang. "Physically Unclonable Functions (PUFs): A New Frontier in Supply Chain Product and Asset Tracking." *IEEE Engineering Management Review*, vol. 49, no. 2 (2021): 116-125.
- [DBL 2019] De Benedictis, Marco, and Antonio Liroy. "A proposal for trust monitoring in a Network Functions Virtualisation Infrastructure." In *2019 IEEE Conference on Network Softwarization (NetSoft)*, pp. 1-9. IEEE, 2019.
- [De Clercq 2002] De Clercq, Jan. "Single sign-on architectures." In *International Conference on Infrastructure Security*, pp. 40-58. Springer, Berlin, Heidelberg, 2002.
- [Deere 2018] Deere, Stephen. "Confidential report: Atlanta's cyber attack could cost taxpayers \$17 million." *The Atlanta Journal—Constitution (Online)*, August 1 (2018).
- [DGR 2015] DiRenzo, Joseph, Dana A. Goward, and Fred S. Roberts. "The little-known challenge of maritime cyber security." In *2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA)*, pp. 1-5. IEEE, 2015.
- [DMK 2020] Deepika, Deepika, Rajnesh Malik, Saurabh Kumar, Rishabh Gupta, and Ashutosh Kumar Singh. "A Review on Data Privacy using Attribute-Based Encryption." In *Proceedings of the International Conference on Innovative Computing & Communications (ICICC)*. 2020.
- [DNV GL 2020] DNV GL. Digitalization in the maritime industry. Accessed November, 2021. <https://www.dnvgl.com/maritime/insights/topics/digitalization-in-the-maritime-industry/index.html>
- [DNV GL 2016] DNV-GL-RP-0496. Cyber security resilience management for ships and mobile offshore units in operation. Accessed November, 2021. <https://www.dnv.com/maritime/dnvgl-rp-0496-recommended-practice-cyber-security-download.html>
- [DSL 2018] Davenport, Amanda, Sachin Shetty, and Xueping Liang. "Attack surface analysis of permissioned blockchain platforms for smart cities." In *2018 IEEE International Smart Cities Conference (ISC2)*, pp. 1-6. IEEE, 2018.
- [DUS+ 2012] Daryabar, Farid, Ali Dehghantanha, Nur Izura Udzir, and Solahuddin bin Shamsuddin. "Towards secure model for SCADA systems." In *Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, pp. 60-64. IEEE, 2012.
- [DW 2014] Duncan, Bob, and Mark Whittington. "Compliance with standards, assurance and audit: does this equal security?." In *Proceedings of the 7th International Conference on Security of Information and Networks*, pp. 77-84. 2014.

[EBS 2018] Edinburgh Business School. "Privacy by Design and Data Protection Impact Assessment (DPIA) Toolkit." December, 2018. Accessed November, 2021. <https://www.hw.ac.uk/documents/privacy-by-design-dpia-toolkit.pdf>

[EC 2014] Council of the EU, General Secretariat of the Council, The EU Maritime Security Strategy (EUMSS), 11205/14, 24.06.2014. June 2014. Accessed November, 2021. <https://data.consilium.europa.eu/doc/document/ST%2011205%202014%20INIT/EN/pdf>

[EC 2018] European Commission. "Maritime: What do we want to achieve?" Mobility and Transport.

[EC 2019] European Commission report 2016-2019, Maritime Affairs and Fisheries, What is the Blue Economy?

[EC 2020A] European Commission, "Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade." December 2020. Accessed November, 2021. <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0>

[EC 2020B] European Commission, "Maritime Security Strategy." Accessed November, 2021. [https://ec.europa.eu/oceans-and-fisheries/ocean/blue-economy/other-sectors/maritime-security-strategy\\_en](https://ec.europa.eu/oceans-and-fisheries/ocean/blue-economy/other-sectors/maritime-security-strategy_en)

[EC 2020C] European Commission, "European Commission Encourages a Maritime Future Which includes Autonomous and Sustainable Ships and Shipping." November 2020. Accessed November, 2021. [https://transport.ec.europa.eu/news/european-commission-encourages-maritime-future-which-includes-autonomous-and-sustainable-ships\\_en](https://transport.ec.europa.eu/news/european-commission-encourages-maritime-future-which-includes-autonomous-and-sustainable-ships_en)

[EC725 2004] EUROPEAN PARLIAMENT AND COUNCIL. IN: Official Journal of the European Union 2004 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004R0725&rid=7>

[ECPSC 2017] European Political Strategy Centre, "Building an Effective European Cyber Shield: Talking EU Cooperation to the Next Level." European Political Strategy Centre. May 2017. Accessed November, 2021. <https://op.europa.eu/en/publication-detail/-/publication/bec56411-5ae4-11e7-954d-01aa75ed71a1/language-en>

[ECS+ 2015] Everspaugh, Adam, Rahul Chaterjee, Samuel Scott, Ari Juels, and Thomas Ristenpart. "The Pythia {PRF} Service." In *24th {USENIX} Security Symposium ({USENIX} Security 15)*, pp. 547-562. 2015.

[EDPS 2019] European Data Protection Supervisor, "EDPS opinion on privacy in the digital age: 'Privacy by Design' as a key tool to ensure citizens' trust in ICTs." March 2010. Accessed November, 2021. [https://ec.europa.eu/commission/presscorner/detail/en/EDPS\\_10\\_6](https://ec.europa.eu/commission/presscorner/detail/en/EDPS_10_6)

[EISAC 2016] Case, Defense Use. "Analysis of the cyber attack on the Ukrainian power grid." *Electricity Information Sharing and Analysis Center (E-ISAC)* 388 (2016).

[El Emam 2008] El Emam, Khaled, and Fida Kamal Dankar. "Protecting privacy using k-anonymity." *Journal of the American Medical Informatics Association* 15, no. 5 (2008): 627-637.

[EMSA 2020A] European Maritime Safety Agency (EMSA), SafeSeaNet main page. Accessed November, 2021. <http://www.emsa.europa.eu/ssn-main.html>

[EMSA 2020B] EMSA. "COVID-19 – Impact on shipping." Accessed November, 2021. <http://emsa.europa.eu/newsroom/covid19-impact/download/6306/4055/23.html>

[ENISA 2011] Cimpean, Dan, Johan Meire, Vincent Bouckaert, Stijn Vande Castele, Aurore Pelle, and Luc Hellebooge. "Analysis of cyber security aspects in the maritime sector." (2011).

[ENISA 2014] ENISA. "Secure ICT Procurement in Electronic Communications." December 2014. Accessed November, 2021. <https://www.enisa.europa.eu/publications/secure-ict-procurement-in-electronic-communications/>

[ENISA 2015] ENISA. "Supply Chain Integrity: An overview of the ICT supply chain risks and challenges, and vision for the way forward." September 2015. Accessed November, 2021. <https://www.enisa.europa.eu/publications/sci-2015>

[ENISA 2017] ENISA. "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures." November 2017. Accessed November, 2021. <https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot>

[ENISA 2017A] ENISA. "Communication network dependencies for ICS/SCADA Systems." February 2017. Accessed November, 2021. <https://www.enisa.europa.eu/publications/ics-scada-dependencies>

[ENISA 2018] ENISA. "Good Practices for Security of Internet of Things, in the context of Smart Manufacturing." November 2018. Accessed November, 2021. <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot>

[ENISA 2019] ENISA. "Port cybersecurity-good practices for cybersecurity in the maritime sector." November 2019. Accessed November, 2021. <https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector>

[ENISA 2019A] ENISA. "Industry 4.0 Cybersecurity: Challenges & Recommendations." May 2019. Accessed November, 2021. <https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations>

[ENISA 2020] ENISA. "Inventory of Risk Management / Risk Assessment Method." Accessed November, 2021. <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods>

[ENISA 2020B] ENISA. "ENISA Threat Landscape – 2020." December 2020. Accessed November, 2021. <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/enisa-threat-landscape-2020>

[ENISA 2020C] ENISA. "Guidelines for Securing the Internet of Things." November 2009. Accessed November, 2021. <https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things>

[ENISA 2020D] ENISA. "Standardisation in support of the Cybersecurity Certification." February 2020. Accessed November, 2021. <https://www.enisa.europa.eu/publications/recommendations-for-european-standardisation-in-relation-to-csa-i>

[ENISA 2020E] ENISA. Drougkas, Athanasios, Anna Sarri, Pinelopi Kyranoudi. "Cyber Risk Management for Ports. Guidelines for cybersecurity in the maritime sector." December, 2020.

[ENISA 2021A] ENISA. "Methodology for sectoral cybersecurity assessments." EU Cybersecurity Certification Framework, September 2021. Accessed November, 2021. <https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment>

[ENISA 2021B] ENISA. "Cybersecurity Challenges in the Uptake of Artificial Intelligence in Autonomous Driving." February 2021. Accessed November, 2021. <https://www.enisa.europa.eu/news/enisa-news/cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving>

[ENISA 2021C] ENISA. "Threat Landscape 2021. " October 2021. Accessed November, 2021. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>

[EPCCert 2010] EPCGlobal. "EPCGlobal Certificate Profile Specification. " June 2010. Accessed November, 2021. [https://www.gs1.org/sites/default/files/docs/cert/cert\\_2\\_0-standard-20100610.pdf](https://www.gs1.org/sites/default/files/docs/cert/cert_2_0-standard-20100610.pdf)

[EPRS 2020] European Parliamentary Research Service. Madiega ,Tambiama. "Digital sovereignty for Europe." PE 651.992, July 2020. Accessed November, 2021. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS\\_BRI\(2020\)651992\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf)

[Ercan 2007] Nergiz, Mehmet Ercan, Maurizio Atzori, and Chris Clifton. "Hiding the presence of individuals from shared databases." In *Proceedings of the 2007 ACM SIGMOD international conference on Management of data*, pp. 665-676. 2007.

[Ericson 1999] Ericson, Clifton A. "Fault tree analysis." In *System Safety Conference, Orlando, Florida*, vol. 1, pp. 1-9. 1999.

[EU 881/19 2019] Regulation (EU) 2019/881 (April 17, 2019) of the European Parliament and of the Council, (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Accessed November, 2021. <https://eur-lex.europa.eu/eli/reg/2019/881/oj>

[EU 2020] European Union. Blue Growth. Accessed November, 2021. [https://ec.europa.eu/maritimeaffairs/policy/blue\\_growth\\_en](https://ec.europa.eu/maritimeaffairs/policy/blue_growth_en)

[Europol 2020] Europol. "Internet Organized Threat Assessment." October, 2020. Accessed November, 2021. <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020>

[Europol 2021] Europol. "Internet Organized Threat Assessment." October, 2021. Accessed November, 2021. <https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021>

[FAK+ 2014] Fremantle, Paul, Benjamin Aziz, Jacek Kopecký, and Philip Scott. "Federated identity and access management for the internet of things." In *2014 International Workshop on Secure Internet of Things*, pp. 10-17. IEEE, 2014.

[FCK 2017] Ficco, Massimo, Michał Choraś, and Rafał Kozik. "Simulation platform for cyber-security and vulnerability analysis of critical infrastructures." *Journal of computational science* 22 (2017): 179-186.

[Feuerlicht 2011] Feuerlicht, George. "E-business interoperability: Challenges and opportunities." In *Proceedings of the International Conference on e-Business*, pp. 1-6. IEEE, 2011.

[FHS 2020] Healthcare Cybersecurity Horizon Report, 2020. Fortified Health Security. Accessed November, 2021. <https://fortifiedhealthsecurity.com/wp-content/uploads/2019/12/Fortified-Health-Security-2020-Horizon-Report.pdf>

[FKS+ 2020] Furumoto, Keisuke, Antti Kolehmainen, Bilhanan Silverajan, Takeshi Takahashi, Daisuke Inoue, and Koji Nakao. "Toward automated smart ships: Designing effective cyber risk management." In *2020 International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics)*, pp. 100-105. IEEE, 2020.

[FLN] Family Links Network. Template for Data Protection Impact Assessment (DPIA). Accessed November, 2021. [https://iapp.org/media/pdf/resource\\_center/dpia-template.pdf](https://iapp.org/media/pdf/resource_center/dpia-template.pdf)

[FMI+ 2005] Freedman, Michael J., Yuval Ishai, Benny Pinkas, and Omer Reingold. "Keyword search and oblivious pseudorandom functions." In *Theory of Cryptography Conference*, pp. 303-324. Springer, Berlin, Heidelberg, 2005.

[FMP+ 2018] Foglietta, Chiara, Dario Masucci, Cosimo Palazzo, Riccardo Santini, Stefano Panzieri, Luis Rosa, Tiago Cruz, and Leonid Lev. "From detecting cyber-attacks to mitigating risk within a hybrid environment." *IEEE Systems Journal* 13, no. 1 (2018): 424-435.

[FMZ 2021] Fan, Cunlong, Jakub Montewka, and Di Zhang. "Towards a Framework of Operational-Risk Assessment for a Maritime Autonomous Surface Ship." *Energies* 14, no. 13 (2021): 3879.

[Frederiksen 2021] Tore Frederiksen. 2021. A Holistic Approach to Enhanced Security and Privacy in Digital Health Passports. In *The 16th International Conference on Availability, Reliability and Security (ARES 2021)*. Association for Computing Machinery, New York, NY, USA, Article 133, 1–10. DOI:<https://doi.org/10.1145/3465481.3469212>

[FS 2018] Ferrara, Pietro, and Fausto Spoto. "Static Analysis for GDPR Compliance." In *ITASEC*. 2018.

[FSS+ 2017] Ferreira, Hugo, Filipe Silva, Pedro Sousa, Bruno Matias, André Faria, Joel Oliveira, José Miguel Almeida, Alfredo Martins, and Eduardo Silva. "Autonomous systems in remote areas of the ocean using BLUECOM+ communication network." In *OCEANS 2017-Anchorage*, pp. 1-6. IEEE, 2017.

[FWM+ 2020] Fan, Cunlong, Krzysztof Wróbel, Jakub Montewka, Mateusz Gil, Chengpeng Wan, and Di Zhang. "A framework to identify factors influencing navigational risk for Maritime Autonomous Surface Ships." *Ocean Engineering* 202 (2020): 107188.

[Gagniuc 2017] Gagniuc, Paul A. *Markov chains: from theory to implementation and experimentation*. John Wiley & Sons, 2017.

[GBS+ 2021] Grigoriadis, Christos, Adamandios Berzovitis, Ioannis Stellos and Panayiotis Kotzanikolaou. "A Cybersecurity Ontology to Support Risk Information Gathering in Cyber-Physical Systems." In 7th Workshop on the Security of Industrial Control Systems & of Cyber-Physical Systems (CyberICPS 2021). October 2021

[GF 2019] Giuliano, Vincenzo, and Valerio Formicola. "ICSrange: A simulation-based cyber range platform for industrial control systems." *arXiv preprint arXiv:1909.01910* (2019).

[GGK+ 2020] Gope, Prosanta, Youcef Gheraibia, Sohag Kabir, and Biplab Sikdar. "A secure IoT-based modern healthcare system with fault-tolerant decision making process." *IEEE Journal of Biomedical and Health Informatics* 25, no. 3 (2020): 862-873.

[GH 2019] Ghaffarinia, Masoud, and Kevin W. Hamlen. "Binary control-flow trimming." In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1009-1022. 2019.

[GJL 2020] Golan, Maureen S., Laura H. Jernegan, and Igor Linkov. "Trends and applications of resilience analytics in supply chain modeling: systematic literature review in the context of the COVID-19 pandemic." *Environment Systems and Decisions* 40 (2020): 222-243.

[GKH+ 2020] Gonczol, Peter, Panagiota Katsikouli, Lasse Herskind, and Nicola Dragoni. "Blockchain implementations and use cases for supply chains-a survey." *Ieee Access* 8 (2020): 11856-11871.

[GKK+ 2019] Guzman, NH Carreras, D. Kwame Minde Kufoalor, Igor Kozine, and Mary Ann Lundteigen. "Combined safety and security risk analysis using the UFOI-E method: A case study of an autonomous surface vessel." In *Proceedings of the 29th European Safety and Reliability Conference, Lower Saxony, Germany*, pp. 22-26. 2019.

[GM 2019] Germond Basil and Mazaris D. Antonios. "Climate Change and Maritime Security" In *Marine Policy*, Vol.99, Elsevier, pp. 26-266. 2019

[GOLD 2021] Goldblum, M. et al. "Dataset security for machine learning: Data poisoning, backdoor attacks, and defenses." *arXiv preprint arXiv:2012.10544* (2021).

[GPK+ 2021] Grigoriadis, Christos, Spyridon Papastergiou, Panayiotis Kotzanikolaou, Christos Douligeris, Antreas Dionysiou, Athanasopoulos Elias, Karin Bernsmed, Per Hakon Meland, and Liina Kamm. "Integrating and Validating Maritime Transport Security Services: Initial results from the CS4EU demonstrator." In *2021 Thirteenth International Conference on Contemporary Computing (IC3-2021)*, pp. 371-377. 2021.

[GPS+ 2006] Goyal, Vipul, Omkant Pandey, Amit Sahai, and Brent Waters. "Attribute-based encryption for fine-grained access control of encrypted data." In *Proceedings of the 13th ACM conference on Computer and communications security*, pp. 89-98. 2006.

[GPV 2019] Gawanmeh, Amjad, Sazia Parvin, Sitalakshmi Venkatraman, Tony de Souza-Daw, James Kang, Samuel Kaspi, and Joanna Jackson. "A Framework for Integrating Big Data Security Into Agricultural Supply Chain." In *2019 IEEE Fifth International Conference on Big Data Computing Service and Applications (BigDataService)*, pp. 191-194. IEEE, 2019.

[GPX 2021] Vasileios Grammatopoulos, Athanasios, Ilias Politis, and Christos Xenakis. "A web tool for analyzing FIDO2/WebAuthn Requests and Responses." In *The 16th International Conference on Availability, Reliability and Security*, pp. 1-10. 2021.

[Granger 2001] Granger, Sarah. "Social engineering fundamentals, part I: hacker tactics." *Security Focus*, December 18 (2001).

[GS 2020] Gope, Prosanta, and Biplab Sikdar. "An efficient privacy-preserving authenticated key agreement scheme for edge-assisted internet of drones." *IEEE Transactions on Vehicular Technology* 69, no. 11 (2020): 13621-13630.

[GSC+ 2017] Giraldo, Jairo, Esha Sarkar, Alvaro A. Cardenas, Michail Maniatakos, and Murat Kantarcioglu. "Security and privacy in cyber-physical systems: A survey of surveys." *IEEE Design & Test* 34, no. 4 (2017): 7-17.

[GTBS 2021] García-Rodríguez, J., Torres Moreno, R., Bernal Bernabé, J and Skarmeta, A. 2021. Towards a standardized model for privacy-preserving Verifiable Credentials. In *The 16th International Conference on Availability, Reliability and Security (ARES 2021)*. Association for Computing Machinery, New York, NY, USA, Article 126, 1–6. DOI:<https://doi.org/10.1145/3465481.3469204>

[GUG 2021] Guggenberger, T., Schlatt, V., Schmid, J., and N. Urbach. "A structured overview of attacks on blockchain systems." *Proceedings of the Pacific Asia Conference on Information Systems* (2021).

[Gueham 2017] Gueham, Farid. "Digital Sovereignty-Steps Towards a New System of Internet Governance." *Paris: Fondapol* (2017).

[HAA 2021] van Haastrecht, M., Golpur, G., Tzismadia, G., Kab, R., Priboi, C., David, D., Răcățăian, A., Brinkhuis, M., and M. Spruit. "A Shared Cyber Threat Intelligence Solution for SMEs." *MDPI Electronics* 10, no. 23 (2021): 2913.

[Hardt 2012] Hardt, Dick. "The OAuth 2.0 authorization framework." RFC 6749 (2012).

[Hastings 1970] Hastings, W. Keith. "Monte Carlo sampling methods using Markov chains and their applications." (1970): 97-109.

[HHKSR 2017] Höyhty, Marko, Jyrki Huusko, Markku Kiviranta, Kenneth Solberg, and Juha Rokka. "Connectivity for autonomous ships: Architecture, use cases, and research challenges." In *2017 International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 345-

[HAP+ 2016] Hosseinpour, Farhoud, Payam Vahdani Amoli, Juha Plosila, Timo Hämäläinen, and Hannu Tenhunen. "An intrusion detection system for fog computing and IoT based logistic systems using a smart data approach." *International Journal of Digital Content Technology and its Applications* 10 (2016).

[HCG+ 2020] Hassija, Vikas, Vinay Chamola, Vatsal Gupta, Sarthak Jain, and Nadra Guizani. "A survey on supply chain security: Application areas, security threats, and solution architectures." *IEEE Internet of Things Journal* 8, no. 8 (2020): 6222-6246.

[HH 2019] Hintemann, Ralph, and Simon Hinterholzer. "Energy consumption of data centers worldwide." In *The 6th International Conference on ICT for Sustainability (ICT4S)*. Lappeenranta. 2019.

[HH 2011] Hammer-Lahav, Eran and Dick Hardt (2011). "The oauth2.0 authorization protocol. " (2011). Accessed November, 2021. <https://tools.ietf.org/html/draft-ietf-oauth-v2-22>

[HHK+ 2017] Höyhty, Marko, Jyrki Huusko, Markku Kiviranta, Kenneth Solberg, and Juha Rokka. "Connectivity for autonomous ships: Architecture, use cases, and research challenges." In *2017 International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 345-350. IEEE, 2017.

[HK 2019] Haböck, Ulrich, and Stephan Krenn. "Breaking and Fixing Anonymous Credentials for the Cloud." In *International Conference on Cryptology and Network Security*, pp. 249-269. Springer, Cham, 2019.

[HKK+ 2018] Hölbl, Marko, Marko Kompara, Aida Kamišalić, and Lili Nemeč Zlatolas. "A systematic review of the use of blockchain in healthcare." *Symmetry* 10, no. 10 (2018): 470.

[HKN+ 2015] Hasegawa, Keisuke, Naoki Kanayama, Takashi Nishide, and Eiji Okamoto. "Software Implementation of Ciphertext-Policy Functional Encryption with Simple Usability." In *2015 5th International Conference on IT Convergence and Security (ICITCS)*, pp. 1-4. IEEE, 2015.

[HKN+ 2016] Hasegawa, Keisuke, Naoki Kanayama, Takashi Nishide, and Eiji Okamoto. "Software library for ciphertext/key-policy functional encryption with simple usability." *Journal of Information Processing* 24, no. 5 (2016): 764-771.

[HKRW 2021] Helminger, Lukas, Daniel Kales, Sebastian Ramacher, and Roman Walch. "Multi-party Revocation in Sovrin: Performance through Distributed Trust." In *Cryptographers' Track at the RSA Conference*, pp. 527-551. Springer, Cham, 2021.

[HM 2020] Höyhty, Marko, and Jussi Martio. "Integrated satellite–terrestrial connectivity for autonomous ships: Survey and future research directions." *Remote Sensing* 12, no. 15 (2020): 2507.

[HNC+ 2012] Hiser, Jason, Anh Nguyen-Tuong, Michele Co, Matthew Hall, and Jack W. Davidson. "ILR: Where'd my gadgets go?." In *2012 IEEE Symposium on Security and Privacy*, pp. 571-585. IEEE, 2012.

[Hobson 2020] Francesca Hobson. "50% of enterprises and system integrators say it is impossible to comply with the GDPR without a centralised identity management solution." September 2017. Accessed November, 2021. <https://www.ubisecure.com/news-events/organisations-say-gdpr-compliance-impossible-without->

[HOM+ 2017] Höyhty, Marko, Tiia Ojanperä, Jukka Mäkelä, Sami Ruponen, and Pertti Järvensivu. "Integrated 5G satellite-terrestrial systems: Use cases for road safety and autonomous ships." In *Proceedings of the 23rd Ka and Broadband Communications Conference, Trieste, Italy*, pp. 16-19. 2017.

[HP 2020] Hébant, Chloé, and David Pointcheval. "Traceable Attribute-Based Anonymous Credentials." *IACR Cryptol. ePrint Arch.* 2020 (2020): 657.

[HPNK+ 2020] Hinch, Robert, Will Probert, Anel Nurtay, Michelle Kendall, Chris Wymant, Matthew Hall, Katrina Lythgoe, Ana Bulas Cruz, Lele Zhao, Andrea Stewart, Luca Ferretti, Michael Parker, Ares Meroueh, Bryn Mathias, Scott Stevenson, Daniel Montero, James Warren, Nicole K Mather, Anthony Finkelstein, Lucie Abeler-Dörner, David Bonsall and Christophe Fraser. "Effective Configurations of a Digital Contact Tracing App: A report to NHSX." April 2020. Accessed November, 2021. [https://cdn.theconversation.com/static\\_files/files/1009/Report\\_-\\_Effective\\_App\\_Configurations.pdf?1587531217](https://cdn.theconversation.com/static_files/files/1009/Report_-_Effective_App_Configurations.pdf?1587531217)

[HR 2020] Hegde, Jeevith, and Børge Rokseth. "Applications of machine learning methods for engineering risk assessment—A review." *Safety science* 122 (2020): 104492.

[HRK 2019] Hackius, Niels, Sven Reimers, and Wolfgang Kersten. "The privacy barrier for blockchain in logistics: first lessons from the port of Hamburg." In *Logistics Management*, pp. 45-61. Springer, Cham, 2019.

[HS 2012] Horrow, Susmita, and Anjali Sardana. "Identity management framework for cloud based internet of things." In *Proceedings of the First International Conference on Security of Internet of Things*, pp. 200-203. 2012.

[HS 2021] Hanzlik, Lucjan, and Daniel Slamanig. "With a Little Help from My Friends: Constructing Practical Anonymous Credentials." In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pp. 2004-2023. 2021.

[HSE 2018] Seppänen, H., Luukkala, P., Zhang, Z., Torkki, P., and K. Virrantaus. "Critical infrastructure vulnerability – A method for identifying the infrastructure service failure interdependencies." *International Journal of Critical Infrastructure Protection* 22 (2018): 25-38.

[HSMC 2020] David M. Higgins II, P. "New research: An average person has more passwords than an average pop song has words." *The Southern Maryland Chronicle*. February 2020. Accessed November, 2021. <https://southernmarylandchronicle.com/2020/02/26/new-research-an-average-person-has-more-passwords-than-an-average-pop-song-has-words/>

[IACS 2020] IACS Rec. 2020/Corr.1 2020. Rec 166. "Recommendation on Cyber Resilience." July 2020. Accessed November, 2021. <http://www.iacs.org.uk/publications/recommendations/161-180>

[IATF16949 2016] IATF. "Quality Management System Requirements for Automotive Production and Relevant Service Parts Organization." October 2016. Accessed November, 2021. <https://www.aiag.org/quality/iatf16949>

[ICL] Imperial College London - Data protection impact assessments. "Data Protection Impact Assessment Template (WORD)." Accessed November, 2021. <https://www.imperial.ac.uk/admin-services/secretariat/information-governance/data-protection/processing-personal-data/data-assessments/>

[ICO] Information Commissioner's Office. "Data protection impact assessments." Accessed November, 2021. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>

[IHO 2015] IHO. "IHO Data Protection Scheme." Edition 1.2.0, IHO Publication S-63, International Hydrographic Bureau, Monaco. January 2015. Accessed November, 2021. [https://iho.int/uploads/user/Services%20and%20Standards/ENC\\_ECDIS/data\\_protection/S-63\\_e1.2.0\\_EN\\_Jan2015.pdf](https://iho.int/uploads/user/Services%20and%20Standards/ENC_ECDIS/data_protection/S-63_e1.2.0_EN_Jan2015.pdf)

[ILW 2006] Ijure, Vinay M., Sean A. Laughter, and Ronald D. Williams. "Security issues in SCADA networks." *computers & security* 25, no. 7 (2006): 498-506.

[INTEL 2007] Casey, Timothy - INTEL. "Threat agent library helps identify information security risks." *Intel White Paper 2* (2007).

[IMO 2003] International Maritime Organization. "International Convention for the Safety of Life at Sea (SOLAS)." Chapter XI-2 2003. Accessed November, 2021. [https://www.imo.org/en/About/Conventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-\(SOLAS\),-1974.aspx](https://www.imo.org/en/About/Conventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx)

[IMO 2004] International Maritime Organization. SOLAS, Consolidated Edition, 2004: "Consolidated Text of the International Convention for the Safety of Life at Sea." Accessed November, 2021. [http://library.arcticportal.org/1696/1/SOLAS\\_consolidated\\_edition2004.pdf](http://library.arcticportal.org/1696/1/SOLAS_consolidated_edition2004.pdf)

[IMO 2017A] International Maritime Organization. "List of certificates and documents required to be carried on board ships." FAL.2/Circ.131. July 2017. Accessed November, 2021. <https://www.register-iri.com/wp-content/uploads/FAL.2-CIRC.131.pdf>

[IMO 2017B] International Maritime Organization. "Guidelines on Maritime cyber risk management." MSC-FAL.1/Circ.3. July 2017. Accessed November, 2021. <https://www.samgongustofa.is/media/english/MSC-FAL.1-Circ.3---Guidelines-On-Maritime-Cyber-Risk-Management--Secretariat-.pdf>

[IMO 2017C] International Maritime Organization. "Maritime Cyber Risk Management in Safety Management Systems." MSC 98/23/Add.1, Annex 10. June 2017. Accessed November, 2021. [https://www.wcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428\(98\).pdf](https://www.wcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf)

[IMO 2019] International Maritime Organization, "Interim Guidelines for MASS Trials." MSC.1/Circ.1604. June 2019. Accessed November, 2021. <https://www.register-iri.com/wp-content/uploads/MS.1-Circ.1604.pdf>

[IMO 2020] International Maritime Organization. Long-Range Identification and Tracking System - Technical Documentation." MSC.1/Circ.1259/Rev.8. MSC.1/Circ.1294/Rev.6. April 2020. Accessed November, 2021. <https://www.wcdn.imo.org/localresources/en/OurWork/Safety/Documents/LRIT/1259-Rev.8.pdf> <https://www.wcdn.imo.org/localresources/en/OurWork/Safety/Documents/LRIT/1294-Rev.6.pdf>

[IMO 2021] International Maritime Organization. "Outcome of the Regulatory Scoping Exercise for the Use of Maritime Autonomous Surface Ships." June 2021. Accessed November, 2021.

[https://wwwcdn.imo.org/localresources/en/MediaCentre/PressBriefings/Documents/MSC.1-Circ.1638%20-%20Outcome%20of%20The%20Regulatory%20Scoping%20ExerciseFor%20The%20Use%20of%20Maritime%20Autonomous%20Surface%20Ships...%20\(Secretariat\).pdf](https://wwwcdn.imo.org/localresources/en/MediaCentre/PressBriefings/Documents/MSC.1-Circ.1638%20-%20Outcome%20of%20The%20Regulatory%20Scoping%20ExerciseFor%20The%20Use%20of%20Maritime%20Autonomous%20Surface%20Ships...%20(Secretariat).pdf)

[INMARSAT 2021] Inmarsat. "Best Practice Information and Communications Technology (ICT) Recommendations." Accessed November, 2021. <https://www.inmarsat.com/en/insights/maritime/2019/best-practice-ict-guide.html>

[IP Bank 2015] IP Bank B.V., CGE Risk Management Solutions B.V., The next generation BowTie methodology Tool. Rev.15, 2015.

[ISO20858 2007] ISO. ISO 20858:2007: "Ships and marine technology – Maritime port facility security assessments and security plan development." October 2007. Accessed November, 2021. <https://www.iso.org/standard/46051.html>

[ISO/IEC15408-1 2009] ISO. ISO/IEC 15408-1:2009: "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model." December 2009. Accessed November, 2021. <https://www.iso.org/standard/50341.html>

[ISO/IEC27000 2018] ISO. ISO/IEC 27000:2018: Information technology – Security techniques – Information security management systems – Overview and vocabulary." February 2018. Accessed November, 2021. <https://www.iso.org/standard/73906.html>

[ISO/IEC27001 2013] ISO. ISO/IEC 27001:2013: "Information technology – Security techniques – Information security management systems – Requirements." October 2013. Accessed November, 2021. <https://www.iso.org/standard/54534.html>

[ISO/IEC27002 2013] ISO. ISO/IEC 27002:2013: "Information technology – Security techniques – Code of practice for information security controls." October 2013. Accessed November, 2021. <https://www.iso.org/standard/54533.html>

[ISO/IEC27005 2018] ISO. ISO/IEC 27005:2018: "Information technology — Security techniques — Information security risk management." July 2018. Accessed November, 2021. <https://www.iso.org/standard/75281.html>

[ISO/IEC27035 2016] ISO, 27035:2016+: Information technology — Security techniques — Information security incident management, <https://www.iso27001security.com/html/27035.html> (accessed: December 2021)

[ISO/IEC20243-1 2018] ISO. ISO/IEC 20243-1:2018: "Information technology - Open Trusted Technology Provider™ Standard (O-TTPS) - Mitigating maliciously tainted and counterfeit products - Part 1: Requirements and recommendations." February 2018. Accessed November, 2021. <https://www.iso.org/standard/74399.html>

[ISO 2019] ISO. ISO 28000:2007: "Specification for security management systems for the supply chain." September 2007. Accessed November, 2021. <https://www.iso.org/standard/44641.html>

- [ISO31000 2018] ISO. ISO 31000:2018: "Risk Management – Guidelines." February 2018. Accessed November, 2021. <https://www.iso.org/standard/65694.html>
- [ISO/IEC31010 2019] ISO. ISO 31010:2019: "Risk management — Risk assessment techniques." June 2019. Accessed November, 2021. <https://www.iso.org/standard/72140.html>
- [JE 2021] Je, J., Jung, J., and S. Choi. "Toward 6G Security: Technology Trends, Threats, and Solutions." *IEEE Communications Standards Magazine*, vol. 5, no. 3 (2021): 64-71.
- [JES 2017] Jensen, Matilde B., Christer W. Elverum, and Martin Steinert. "Eliciting unknown unknowns with prototypes: Introducing prototrials and prototrial-driven cultures." *Design Studies* 49 (2017): 1-31.
- [JK 2011] Jüttner, Uta, and Stan Maklan. "Supply chain resilience in the global financial crisis: an empirical study." *Supply chain management: An international journal* (2011).
- [JRC 2019] Nai-Fovino, Igor, Ricardo Neisse, José Hernández-Ramos, Nineta Polemi, Gian-Luigi Ruzzante, Malgorzata Figwer, and Alessandro Lazari. "A Proposal for a European Cybersecurity Taxonomy." *Publications Office of the European Union* (2019).
- [JRL+ 2018] Jelacic, Bojan, Daniela Rosic, Imre Lendak, Marina Stanojevic, and Sebastijan Stoja. "STRIDE to a secure smart grid in a hybrid cloud." In *Computer Security*, pp. 77-90. Springer, Cham, 2017.
- [JSS+ 2021] Jubur, Mohammed, Prakash Shrestha, Nitesh Saxena, and Jay Prakash. "Bypassing Push-based Second Factor and Passwordless Authentication with Human-Indistinguishable Notifications." In *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, pp. 447-461. 2021.
- [KAMZ 2019] Kambourakis, Georgios, Marios Anagnostopoulos, Weizhi Meng, and Peng Zhou, eds. *Botnets: Architectures, Countermeasures, and Challenges*. CRC Press, 2019.
- [KAP+ 2018] Kalogeraki, Eleni-Maria, Dimitrios Apostolou, Nineta Polemi, and Spyridon Papastergiou. "Knowledge management methodology for identifying threats in maritime/logistics supply chains." *Knowledge Management Research & Practice* 16, no. 4 (2018): 508-524.
- [KB 2019] Knoblauch, Dorian, and Christian Banse. "Reducing implementation efforts in continuous auditing certification via an Audit API." In *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, pp. 88-92. IEEE, 2019.
- [KCK+ 2019] Kerdprasop, Nittaya, Kacha Chansilp, Kittisak Kerdprasop, and Paradee Chuaybamroong. "Anomaly detection with machine learning technique to support smart logistics." In *International Conference on Computational Science and Its Applications*, pp. 461-472. Springer, Cham, 2019.
- [KDK 2020] Kavallieratos, Georgios, Vasiliki Diamantopoulou, and Sokratis K. Katsikas. "Shipping 4.0: Security requirements for the cyber-enabled ship." *IEEE Transactions on Industrial Informatics* 16, no. 10 (2020): 6617-6625.

- [KEH 2014] Fatema, Kaniz, Vincent C. Emeakaroha, Philip D. Healy, John P. Morrison, and Theo Lynn. "A survey of cloud monitoring tools: Taxonomy, capabilities and objectives." *Journal of Parallel and Distributed Computing* 74, no. 10 (2014): 2918-2933.
- [KGP 2019] Koo, Hyungjoon, Seyedhamed Ghavamnia, and Michalis Polychronakis. "Configuration-driven software debloating." In *Proceedings of the 12th European Workshop on Systems Security*, pp. 1-6. 2019.
- [KHA 2021] Khan, A. A., Khan, M. M., Khan, K. M., Arshad J., and F. Ahmad. "A blockchain-based decentralized machine learning framework for collaborative intrusion detection within UAVs." *Computer Networks*, vol. 196 (2021): 108217.
- [KK 2019] Kamiya, G., and O. Kvarnström. "Data centres and energy—from global headlines to local headaches." *International Energy Agency* <https://www.iea.org/commentaries/data-centres-and-energy-from-global-headlines-to-local-headaches> (2019).
- [KKG 2018] Kavallieratos, Georgios, Sokratis Katsikas, and Vasileios Gkioulos. "Cyber-attacks against the autonomous ship." In *Computer Security*, pp. 20-36. Springer, Cham, 2018.
- [KKG 2020] Kavallieratos, Georgios, Sokratis Katsikas, and Vasileios Gkioulos. "Cybersecurity and safety co-engineering of cyberphysical systems—a comprehensive survey." *Future Internet* 12, no. 4 (2020): 65.
- [KKN+ 2020] Kumar, Dharmendra, Aamir Hussain Khan, Himanshu Nayyar, and Vinita Gupta. "Cyber Risk Assessment Model for Critical Information Infrastructure." In *2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC)*, pp. 292-297. IEEE, 2020.
- [KLK 2019] Kros, John Francis, Ying Liao, Jon Frederick Kirchoff, and James E. Zemanek Jr. "Traceability in the supply chain." *International Journal of Applied Logistics (IJAL)* 9, no. 1 (2019): 1-22.
- [KKV 2013] Kurapati, Shalini, Gwendolyn L. Kolfshoten, Alexander Verbraeck, Thomas M. Corsi, and Frances Brazier. "Exploring shared situational awareness in supply chain disruptions." In *ISCRAM 2013: Proceedings of the 10th International Conference on Information Systems for Crisis Response and Management, Baden-Baden, Germany, 12-15 may 2013*. ISCRAM, 2013.
- [KKV 2021] Kalinin, Maxim, Vasilij Krundyshev, and Peter Zegzhda. "Cybersecurity Risk Assessment in Smart City Infrastructures." *Machines* 9, no. 4 (2021): 78.
- [KLS 2020] Kumar, Akhil, Rong Liu, and Zhe Shan. "Is blockchain a silver bullet for supply chain management? Technical challenges and research opportunities." *Decision Sciences* 51, no. 1 (2020): 8-37.
- [KLS+ 2017] Krenn, Stephan, Thomas Lorünser, Anja Salzer, and Christoph Striecks. "Towards attribute-based credentials in the cloud." In *International Conference on Cryptology and Network Security*, pp. 179-202. Springer, Cham, 2017.

[KMP+ 2019] Kritikos, Kyriakos, Kostas Magoutis, Manos Papoutsakis, and Sotiris Ioannidis. "A survey on vulnerability assessment tools and databases for cloud-based web applications." *Array* 3 (2019): 100011.

[KPMP 2018] Kalogeraki, Eleni-Maria, Spyridon Papastergiou, Haralambos Mouratidis, and Nineta Polemi. "A novel risk assessment methodology for SCADA maritime logistics environments." *Applied Sciences* 8, no. 9 (2018): 1477.

[KRAB+ 2018] Kumar, Tanesh, Vidhya Ramani, Ijaz Ahmad, An Braeken, Erkki Harjula, and Mika Ylianttila. "Blockchain utilization in healthcare: Key requirements and challenges." In *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pp. 1-7. IEEE, 2018.

[KSP+ 2014] Kuznetsov, Volodymyr, László Szekeres, Mathias Payer, George Candea, R. Sekar, and Dawn Song. "Code-pointer integrity." In *The Continuing Arms Race: Code-Reuse Attacks and Defenses*, pp. 81-116. 2018.

[KTG 2013] Kotzanikolaou, Panayiotis, Marianthi Theoharidou, and Dimitris Gritzalis. "Assessing n-order dependencies between critical infrastructures." *International Journal of Critical Infrastructures* 6 9, no. 1-2 (2013): 93-110.

[LAN 2021] Langås, M., Løfqvist, S., Katt, B., Haugan, T., and M. Gilje Jaatun. "With a Little Help from Your Friends: Collaboration with Vendors During Smart Grid Incident Response Exercises." In *European Interdisciplinary Cybersecurity Conference (2021)*: 46-53.

[Loyds 2016] Lloyds Register. "Cyber-enabled ships." Page 20. July 2016. Accessed November, 2021. <http://info.lr.org/1/12702/2016-07-07/32rrbk>

[LDC 2013] Lambrinos, Lambros, Constantinos Djouvas, and Chrysostomos Chrysostomou. "Applying delay tolerant networking routing algorithms in maritime communications." In *2013 IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*, pp. 1-6. IEEE, 2013.

[LES+ 2017] Lai, Russell WF, Christoph Egger, Dominique Schröder, and Sherman SM Chow. "Phoenix: Rebirth of a cryptographic password-hardening service." In *26th {USENIX} Security Symposium ({USENIX} Security 17)*, pp. 899-916. 2017.

[LFL+ 2020] Luecking, Markus, Christian Fries, Robin Lamberti, and Wilhelm Stork. "Decentralized identity and trust management framework for Internet of Things." In *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 1-9. IEEE, 2020.

[LGP+ 2010] Lin, Hao-Min, Yu Ge, Ai-Chun Pang, and Jaya Shankar Pathmasuntharam. "Performance study on delay tolerant networks in maritime communication environments." In *OCEANS'10 IEEE SYDNEY*, pp. 1-6. IEEE, 2010.

[LIM 2021] Lim, M. K., Li, Y., Wang, C., and M.-L. Tseng. "A literature review of blockchain technology applications in supply chains: A comprehensive analysis of themes, methodologies and industries". *Computers & Industrial Engineering*, vol. 154 (2021): 107133.

[LMP 2013] Labunets, Katsiaryna, Fabio Massacci, and Federica Paci. "An experimental comparison of two risk-based security methods." In 2013 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement, pp. 163-172. IEEE, 2013.

[LOS+ 2010] Lewko, Allison, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters. "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption." In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 62-91. Springer, Berlin, Heidelberg, 2010.

[LP 2018] Li, Chao, and Balaji Palanisamy. "Privacy in Internet of Things: From principles to technologies." *IEEE Internet of Things Journal* 6, no. 1 (2018): 488-505.

[LSC 2015] Lin, Iuon-Chang, Hung-Huei Hsu, and Chen-Yang Cheng. "A cloud-based authentication protocol for RFID supply chain systems." *Journal of Network and Systems Management* 23, no. 4 (2015): 978-997.

[LSH+ 2011] Li, Chunquan, Yuling Shang, Chunyang Hu, and Panfeng Zhu. "Research on Cloud Manufacturing Multi-Granular Resource Access Control Based on Capacity Constraint." *Adv. Inf. Sci. Serv. Sci.* 3, no. 5 (2011): 79-86.

[LSN+ 2020] Lyastani, Sanam Ghorbani, Michael Schilling, Michaela Neumayr, Michael Backes, and Sven Bugiel. "Is FIDO2 the kingslayer of user authentication? A comparative usability study of FIDO2 passwordless authentication." In *2020 IEEE Symposium on Security and Privacy (SP)*, pp. 268-285. IEEE, 2020.

[LSS 2010] Lund, Mass Soldal, Bjørnar Solhaug, and Ketil Stølen. *Model-driven risk analysis: the CORAS approach*. Springer Science & Business Media, 2010.

[LSS 2020] Lund, M. S., Solhaug, B., & Stølen, K. (2010). *Model-driven risk analysis: the CORAS approach*. Springer Science & Business Media. Springer-Verlag, Berlin Heidelberg, ISBN:978-3-642-12323-8.

[M-APP 2020] Munoz-Arcenales, Andres, Sonsoles López-Pernas, Alejandro Pozo, Álvaro Alonso, Joaquín Salvachúa, and Gabriel Huecas. "Data Usage and Access Control in Industrial Data Spaces: Implementation Using FIWARE." *Sustainability* 12, no. 9 (2020): 3885.

[Macola 2020] Ilaria Grasso Macola. "Is COVID-19 accelerating digital engagement in maritime?" September 2020. Accessed November, 2021. <https://www.ship-technology.com/features/is-covid-19-accelerating-digital-engagement-in-maritime/>

[Markatos 2020] Evangelos Markatos (editor) - CyberSec4Europe. Deliverable D4.3 "Research and Development Roadmap 1." January 2020. Accessed November, 2021. <https://cybersec4europe.eu/wp-content/uploads/2020/09/D4.3-Roadmap-v5-NEW.pdf>

[Markatos 2021] Evangelos Markatos (editor) - CyberSec4Europe. Deliverable D4.4 "Research and Development Roadmap 2." January 2021. Accessed November, 2021 <https://cybersec4europe.eu/wp-content/uploads/2021/02/D4.4-Research-and-Development-Roadmap-2-v3.0-submitted.pdf>

- [Martin 2020] Martin, Robert Alan. "Visibility & control: addressing supply chain challenges to trustworthy software-enabled things." In *2020 IEEE Systems Security Symposium (SSS)*, pp. 1-4. IEEE, 2020.
- [MAZ 2021] Mazhar, N., Salleh, R., Zeeshan, M., and M. M. Hameed. "Role of Device Identification and Manufacturer Usage Description in IoT Security: A Survey." *IEEE Access*, vol. 9 (2021): 41757-41786.
- [MBG+ 2020] Torres Moreno, Rafael, Jorge Bernal Bernabe, Jesus Garcia Rodriguez, Tore Kasper Frederiksen, Michael Stausholm, Noelia Martínez, Evangelos Sakkopoulos, Nuno Ponte, and Antonio Skarmeta. "The OLYMPUS Architecture—Oblivious Identity Management for Private User-Friendly Services." *Sensors* 20, no. 3 (2020): 945.
- [MBP+ 2010] Mahalle, Parikshit, Sachin Babar, Neeli R. Prasad, and Ramjee Prasad. "Identity management framework towards internet of things (IoT): Roadmap and key challenges." In *International Conference on Network Security and Applications*, pp. 430-439. Springer, Berlin, Heidelberg, 2010.
- [MBWRN 2021] Meland, P. H., K. Bernsmed, E. Wille, Ø. J. Rødseth, and D. A. Nesheim. "A retrospective analysis of maritime cyber security incidents." In *Proceedings of the 14th international conference on marine navigation and safety of sea transportation*. 2021.
- [McDougall 2017] Allan McDougall. "Security and Safety for Autonomous Ships." *The Maritime Executive*. December 2017. Accessed November, 2021. <https://www.maritime-executive.com/editorials/security-and-safety-management-for-autonomous-ships>
- [MCP 2020] MCP consortium, 2020, Maritime Connectivity Platform (MCP). Accessed November, 2021. <https://maritimeconnectivity.net/>
- [MD 2018] Mouratidis, Haralambos, and Vasiliki Diamantopoulou. "A security analysis method for industrial internet of things." *IEEE Transactions on Industrial Informatics* 14, no. 9 (2018): 4093-4100.
- [MEZ 2020] Matheu, Sara N., Alberto Robles Enciso, Alejandro Molina Zarca, Dan Garcia-Carrillo, José Luis Hernández-Ramos, Jorge Bernal Bernabe, and Antonio F. Skarmeta. "Security architecture for defining and enforcing security profiles in DLT/SDN-based IoT systems." *Sensors* 20, no. 7 (2020): 1882.
- [MFMP 2006] Mellado, Daniel, Eduardo Fernández-Medina, and Mario Piattini. "Applying a security requirements engineering process." In *European Symposium on Research in Computer Security*, pp. 192-206. Springer, Berlin, Heidelberg, 2006.
- [MG 2007] Mouratidis, Haralambos, and Paolo Giorgini. "Secure tropos: a security-oriented extension of the tropos methodology." *International Journal of Software Engineering and Knowledge Engineering* 17, no. 02 (2007): 285-309.
- [MGB+ 2021] Moreno, Rafael Torres, Jesús García-Rodríguez, Jorge Bernal Bernabé, and Antonio Skarmeta. "A Trusted Approach for Decentralised and Privacy-Preserving Identity Management." *IEEE Access* 9 (2021): 105788-105804.
- [MGG 2018] Mühle, Alexander, Andreas Grüner, Tatiana Gayvoronskaya, and Christoph Meinel. "A survey on essential components of a self-sovereign identity." *Computer Science Review* 30 (2018): 80-86.

[MH 2019] Munim, Ziaul Haque. "Autonomous ships: a review, innovative applications and future maritime business models." In *Supply Chain Forum: An International Journal*, vol. 20, no. 4, pp. 266-279. Taylor & Francis, 2019.

[MICROSOFT 2009] Microsoft. "The stride threat model." December 2009. Accessed November, 2021. [https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878\(v=cs.20\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN)

[Min 2019] Min, Hokey. "Blockchain technology for enhancing supply chain resilience." *Business Horizons* 62, no. 1 (2019): 35-45.

[MKL 2021] Lim, M.K., Li, Y., Wang, C., and M.-L.Tseng. "A literature review of blockchain technology applications in supply chains: A comprehensive analysis of themes, methodologies and industries." *Computers & Industrial Engineering*, vol. 154 (2021): 107133.

[MM 2018] MacMillan, Douglas, and Robert MacMillan. "Google exposed user data, feared repercussions of disclosing to public." *Wall Street Journal* 8 (2018).

[MRP 2019] Matheu, Sara Nieves, José Luis Hernández-Ramos, Salvador Pérez, and Antonio F. Skarmeta. "Extending MUD profiles through an automated IoT security testing methodology." *IEEE Access* 7 (2019): 149444-149463.

[MS 2009] Mitnick, Kevin D., and William L. Simon. *The art of intrusion: the real stories behind the exploits of hackers, intruders and deceivers*. John Wiley & Sons, 2009.

[MSR 2019] Markovic-Petrovic, Jasna D., Mirjana D. Stojanovic, and Slavica V. Bostjancic Rakas. "A fuzzy AHP approach for security risk assessment in SCADA networks." *Advances in Electrical and Computer Engineering* 19, no. 3 (2019): 69-74.

[MSW 2006] Simon, William L., Steve Wozniak, and Kevin D. Mitnick. *The Art of Deception: Controlling the Human Element of Security*. Wiley, 2002. Paperback ISBN 0-471-23712-4 (2006).

[MTA 2010] Morris, Bonnie, Cynthia Tanner, and Joseph D'Alessandro. "Enabling trust through continuous compliance assurance." In *2010 Seventh International Conference on Information Technology: New Generations*, pp. 708-713. IEEE, 2010.

[Muffet 2019] Muffet, Alec. "Facebook: Password hashing & authentication." *Presentation at Real World Crypto* (2015).

[MUNIN 2016] MUNIN. Maritime unmanned navigation through intelligence in networks, 2016. Accessed November, 2021. <http://www.unmanned-ship.org/munin/>

[MYL 2021] Mylrea M., Nielsen M., John J., and M. Abbaszadeh. "Digital Twin Industrial Immune System: AI-driven Cybersecurity for Critical Infrastructures." *Systems Engineering and Artificial Intelligence*. Springer, Cham (2021).

[NAD 2021] Nadeem, A., Verwer, S., Moskal, S., and S. J. Yang, "Alert-driven Attack Graph Generation using S-PDFA." *IEEE Transactions on Dependable and Secure Computing*, in press (2021).

[NERC 2017] NERC, Cyber Security — Supply Chain Risk Management, NERC CIP-013-1, July 2017.

[NFW 2017] Nagaraju, Vidhyashree, Lance Fiondella, and Thierry Wandji. "A survey of fault and attack tree modeling and analysis for cyber risk management." In *2017 IEEE International Symposium on Technologies for Homeland Security (HST)*, pp. 1-6. IEEE, 2017.

[NIS DIRECTIVE 2016] EU Council Directive on Network and Information Security. Directive 2016/1148/EU of the European Parliament and of the Council of 6 July 2016 "Concerning measures for a high common level of security of network and information systems across the Union." *Official Journal of the European Union* L194(19.7). July 2016. Accessed November, 2021. <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32016L1148>

[NIS 2 DIRECTIVE 2020] Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, Brussels, 16.12.2020, COM(2020) 823, 2020/0359 (COD). December 2020. Accessed November, 2021. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN>

[NIST 2012] NIST. NIST Special Publication 800-30 R1: "Guide for Conducting Risk Assessments." September 2012. Accessed November, 2021. <https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final>

[NIST 2015] NIST. NIST Special Publication 800-161: "Supply Chain Risk Management. Practices for Federal Information Systems and Organizations." April 2015. Accessed November, 2021. <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-161.pdf>

[NIST 2015B] NIST. NIST Special Publication 800-82: "Guide to Industrial Control Systems (ICS) Security." May 2015. Accessed November, 2021. <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf>

[NIST 2018] NIST. "Framework for Improving Critical Infrastructure Cybersecurity." April 2018. Accessed November, 2021. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

[NIST 2018B] NIST. NIST Special Publication 800-37: "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy." December 2018. Accessed November, 2021. <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-37r1.pdf>

[NIST 2019] NIST. "Cyber Supply Chain Risk Management." Accessed November, 2021. <https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management>

[NIST 2020] NIST. NIST Special Publication 800-55: "Performance Measurement Guide for Information Security." July 2020. Accessed November, 2021. <https://csrc.nist.gov/publications/detail/sp/800-55/rev-1/final>

[NIST 2020c] NIST, Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53, Rev. 5, December 2020.

[NIST 2021] NIST, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, NIST SP 800-161, Rev.1, 2nd Draft, October 2021.

[NISTIR 2021] NIST, NISTIR 8286 "Integrating Cybersecurity and Enterprise Risk Management (ERM)", October 2020. <https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf> (accessed: December 2021)

[NISTIR 2021b] NIST, Draft NISTIR 8374 "Cybersecurity Framework Profile for Ransomware Risk Management", September 2021. <https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8374-draft.pdf> (accessed: December 2021)

[NMH 2009] Narayanan, Sriram, Ann S. Marucheck, and Robert B. Handfield. "Electronic data interchange: research review and future directions." *Decision Sciences* 40, no. 1 (2009): 121-163.

[NNY 2010] Nhlabatsi, Armstrong, Bashar Nuseibeh, and Yijun Yu. "Security requirements engineering for evolving software systems: A survey." In *Security-aware systems applications and software development methods*, pp. 108-128. IGI Global, 2012.

[NPK 2018] Nuss, Martin, Alexander Puchta, and Michael Kunz. "Towards blockchain-based identity and access management for internet of things in enterprises." In *International Conference on Trust and Privacy in Digital Business*, pp. 167-181. Springer, Cham, 2018.

[NV 2017] No, Won Gyun, and Miklos A. Vasarhelyi. "Cybersecurity and continuous assurance." *Journal of Emerging Technologies in Accounting* 14, no. 1 (2017): 1-12.

[NZMZ 2010] Nagarakatte, Santosh, Jianzhou Zhao, Milo MK Martin, and Steve Zdancewic. "CETS: compiler enforced temporal safety for C." In *Proceedings of the 2010 International Symposium on Memory Management*, pp. 31-40. 2010.

[OB 2020] Omar, Ahmad Sghaier, and Otman Basir. "Decentralized Identifiers and Verifiable Credentials for Smartphone Anticounterfeiting and Decentralized IMEI Database." *Canadian Journal of Electrical and Computer Engineering* 43, no. 3 (2020): 174-180.

[O'RLM 2019] O'Raw, John, David Lavery, and D. John Morrow. "Securing the industrial Internet of Things for critical infrastructure (IIoT-CI)." In *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, pp. 70-75. IEEE, 2019.

[ORU 2021] Orue-Echevarria, L., Garcia, J.L., Banse, C. and J. Alonso. "MEDINA: Improving Cloud Services trustworthiness through continuous audit-based certification." First workshop on trustworthy software and open source (2021).

[OSL 2021] Oh, Se-Ra, Young-Duk Seo, Euijong Lee, and Young-Gab Kim. "A Comprehensive Survey on Security and Privacy for Electronic Health Data." *International Journal of Environmental Research and Public Health* 18, no. 18 (2021): 9668.

[PA 2021] Prabhakar, Anjana; Anjali, Tricha. Towards flexible hardware authentication for IoT. In 2021 International Symposium on Networks, Computers and Communications (ISNCC). IEEE. p. 1-6.

[PAN 2020] Panda, A., and A. Bower. "Cyber security and the disaster resilience framework." *International Journal of Disaster Resilience in the Built Environment*, vol. 11, no. 4 (2020).

[Pashchenko+ 2021] Pashchenko, Ivan, Riccardo Scandariato, Antonino Sabetta, and Fabio Massacci. "Secure Software Development in the Era of Fluid Multi-party Open Software and Services." In *2021 IEEE/ACM 43rd International Conference on Software Engineering: New Ideas and Emerging Results (ICSE-NIER)*, pp. 91-95. IEEE, 2021.

[PaX 2003] PaX TEAM, "Address space layout randomization (ASLR)," 2003. Accessed November, 2021. <https://pax.grsecurity.net/docs/aslr.txt>

[PCvdV 2017] Pawlowski, Andre, Moritz Contag, Victor van der Veen, Chris Ouwehand, Thorsten Holz, Herbert Bos, Elias Athanasopoulos, and Cristiano Giuffrida. "MARX: Uncovering Class Hierarchies in C++ Programs." In *NDSS*. 2017.

[PHL+ 2018] Pantazopoulos, Panagiotis, Sammy Haddad, Costas Lambrinoudakis, Christos Kalloniatis, Konstantinos Maliatsos, Athanasios Kanatas, András Varádi, Matthieu Gay, and Angelos Amditis. "Towards a security assurance framework for connected vehicles." In *2018 IEEE 19th International Symposium on "A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*, pp. 01-06.

[PIE 2021] Centobelli, P., Cerchione, R., Del Vecchio, P., Oropallo, E., and G. Secundo. "Blockchain technology for bridging trust, traceability and transparency in circular supply chain." *Information & Management* (2021): 103508.

[PJB+ 2020] Preuveneers, Davy, Wouter Joosen, Jorge Bernal Bernabe, and Antonio Skarmeta. "Distributed Security Framework for Reliable Threat Intelligence Sharing." *Security and Communication Networks* 2020 (2020).

[PKG 2017] Pattakou, Argyri, Christos Kalloniatis, and Stefanos Gritzalis. "Security and privacy requirements engineering methods for traditional and cloud-based systems: a review." *Cloud Comput* 2017 (2017): 155.

[PKP 2016] Papastergiou, Spyridon, Nineta Polemi, and Panayiotis Kotzanikolaou. "Design and validation of the Medusa supply chain risk assessment methodology and system." *International Journal of Critical Infrastructures* 14, no. 1 (2018): 1-39.

[PKP 2020] Pokhrel, Abhishek, Vikash Katta, and Ricardo Colomo-Palacios. "Digital Twin for Cybersecurity Incident Prediction: A Multivocal Literature Review." In *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops*, pp. 671-678. 2020.

[PKP 2021] Papastergiou, Spyridon, Eleni-Maria Kalogeraki, Nineta Polemi, and Christos Douligeris. "Challenges and Issues in Risk Assessment in Modern Maritime Systems." In *Advances in Core Computer Science-Based Technologies*, pp. 129-156. Springer, Cham, 2021.

[PM 2018] Porwal, Shardha, and Sangeeta Mittal. "Design of Concurrent Ciphertext Policy-Attribute Based Encryption Library for Multilevel Access of Encrypted Data." In *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, pp. 42-47. IEEE, 2018.

[POM 2020] Petersen, Stig, Pål Orten, and Bård Myhre. "Potential benefits of 5G communication for autonomous ships." In *IOP Conference Series: Materials Science and Engineering*, vol. 929, no. 1, p. 012009. IOP Publishing, 2020.

[POU 2021] Pournader, M., Ghaderi, H., Hassanzadegan, A. and B. Fahimnia. "Artificial intelligence applications in supply chain management". *International Journal of Production Economics*, vol. 241 (2021): 108250.

[PP 2018] Papastergiou, Spyridon, and Nineta Polemi. "MITIGATE: a dynamic supply chain cyber risk assessment methodology." In *Smart Trends in Systems, Security and Sustainability*, pp. 1-9. Springer, Singapore, 2018.

[PPK 2012] Pappas, Vasilis, Michalis Polychronakis, and Angelos D. Keromytis. "Smashing the gadgets: Hindering return-oriented programming using in-place code randomization." In *2012 IEEE Symposium on Security and Privacy*, pp. 601-615. IEEE, 2012.

[PPK 2015] Papastergiou, Spyridon, Nineta Polemi, and Athanasios Karantjias. "CYSM: an innovative physical/cyber security management system for ports." In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pp. 219-230. Springer, Cham, 2015.

[PPK 2018] Papastergiou, Spyridon, Nineta Polemi, and Panayiotis Kotzanikolaou. "Design and validation of the Medusa supply chain risk assessment methodology and system." *International Journal of Critical Infrastructures* 14, no. 1 (2018): 1-39.

[PPK 2021] Papastergiou, S., Kalogeraki, E. M., Polemi, N., and C. Douligeris. "Challenges and Issues in Risk Assessment in Modern Maritime Systems." In: Tsihrintzis G., Virvou M. (eds) *Advances in Core Computer Science-Based Technologies. Learning and Analytics in Intelligent Systems*, vol 14. Springer, Cham (2021):129-156.

[PPM 2011] Papanikolaou, Nick, Siani Pearson, and Marco Casassa Mont. "Towards natural-language understanding and automated enforcement of privacy rules and regulations in the cloud: survey and bibliography." In *FTRA International Conference on Secure and Trust Computing, Data Management, and Application*, pp. 166-173. Springer, Berlin, Heidelberg, 2011.

[PPW+ 2005] Pye, Graeme, Justin D. Pierce, Matthew Warren, and David Mackay. "Supply chain security: the need for continuous assessment." *Supply Chain Practice* 7, no. 1 (2005): 56-68.

[PR 2005] Permann, May Robin, and Kenneth Rohde. "Cyber assessment methods for SCADA security." In *15th annual joint ISA POWID/EPRI controls and instrumentation conference, Nashville, TN. 2005*.

[PRG+ 2018] Pérez, Salvador, José L. Hernández-Ramos, Sara N. Matheu-García, Domenico Rotondi, Antonio F. Skarmeta, Leonardo Straniero, and Diego Pedone. "A lightweight and flexible encryption scheme to protect sensitive data in smart building scenarios." *IEEE Access* 6 (2018): 11738-11750.

[PS 2008] Panzieri, Stefano, and Roberto Setola. "Failures propagation in critical interdependent infrastructures." *International Journal of Modelling, Identification and Control* 3, no. 1 (2008): 69-78.

[PS 2019] Pinto, Sandro, and Santos, Nuno. "Demystifying Arm TrustZone: A Comprehensive Survey." In *CM Computing Surveys (CSUR)*, 51(6), 1-36.

[PSvS 2019] Prinsloo, Jaco, Saurabh Sinha, and Basie von Solms. "A review of industry 4.0 manufacturing process security risks." *Applied Sciences* 9, no. 23 (2019): 5105.

[Purdy 2021] Andy Purdy. "Why Global Internet Security Standards Can Provide a Foundation For Assurance And Accountability." February 2021. Accessed November, 2021. <https://www.forbes.com/sites/forbestechcouncil/2021/02/19/why-global-internet-security-standards-can-provide-a-foundation-for-assurance-and-accountability>

[PvdB 2017] Voigt, Paul, and Axel Von dem Bussche. "The eu general data protection regulation (gdpr)." *A Practical Guide, 1st Ed., Cham: Springer International Publishing* 10 (2017): 3152676.

[PZ 2013] Paquin, Christian, and Greg Zaverucha. "U-prove cryptographic specification v1. 1." *Technical Report, Microsoft Corporation*. December 2013. Accessed November, 2021. <https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/U-Prove20Cryptographic20Specification20V1.1.pdf>

[PZC+ 2020] Papadamou, Kostantinos, Savvas Zannettou, Bogdan Chifor, Sorin Teican, George Gugulea, Alberto Caponi, Annamaria Recupero et al. "Killing the Password and Preserving Privacy with Device-Centric and Attribute-based Authentication." *IEEE Transactions on Information Forensics and Security* 15 (2019): 2183-2193.

[QHA+ 2019] Qian, Chenxiong, Hong Hu, Mansour Alharthi, Pak Ho Chung, Taesoo Kim, and Wenke Lee. "RAZOR: A framework for post-deployment software debloating." In *28th {USENIX} Security Symposium ({USENIX} Security 19)*, pp. 1733-1750. 2019.

[QPY 2018] Quach, Anh, Aravind Prakash, and Lok Yan. "Debloating software through piece-wise compilation and loading." In *27th {USENIX} Security Symposium ({USENIX} Security 18)*, pp. 869-886. 2018.

[QTB 2019] Queiroz, Maciel M., Renato Telles, and Silvia H. Bonilla. "Blockchain and supply chain management integration: a systematic review of the literature." *Supply Chain Management: An International Journal* (2019).

[RAN 2021] Ranaweera, P., Jurcut A. D., and M. Liyanage. "Survey on Multi-Access Edge Computing Security and Privacy." *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2 (2021): 1078-1124.

[RAR+ 2020] Rubio, Juan E., Cristina Alcaraz, Ruben Rios, Rodrigo Roman, and Javier Lopez. "Distributed detection of apts: consensus vs. clustering." In *European Symposium on Research in Computer Security*, pp. 174-192. Springer, Cham, 2020.

- [RB 2015] Rødseth, Ørnulf Jan, and H-C. Burmeister. "Risk assessment for an unmanned merchant ship." *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation* 9, no. 3 (2015): 357-364.
- [RCD+ 2021] Russo, Margherita, Claudia Cardinale Ciccotti, Fabrizio De Alexandris, Antonela Gjinaj, Giovanni Romaniello, Antonio Scatorchia, and Giorgio Terranova. "A cross-country comparison of contact-tracing apps during COVID-19."
- [RCT+ 2018] Raman, Sudha R., Lesley H. Curtis, Robert Temple, Tomas Andersson, Justin Ezekowitz, Ian Ford, Stefan James et al. "Leveraging electronic health records for clinical research." *American heart journal* 202 (2018): 13-19.
- [RFM+, 2020] Rødseth, Ørnulf Jan, Christian Frøystad, Per Håkon Meland, Karin Bernsmed, and Dag Atle Nesheim. "The need for a public key infrastructure for automated and autonomous ships." In *IOP Conference Series: Materials Science and Engineering*, vol. 929, no. 1, p. 012017. IOP Publishing, 2020.
- [RJ 2016] DK Rasmus, Nord Jorgensen, in Copenhagen. "Bimco: The guidelines on cyber security onboard ships." December 2018. Accessed November, 2021. <https://iumi.com/news/news/bimco-the-guidelines-on-cyber-security-onboard-ships>
- [RKP+ 2013] Rødseth, Ørnulf Jan, Beate Kvamstad, Thomas Porathe, and Hans-Christoph Burmeister. "Communication architecture for an unmanned merchant ship." In *2013 MTS/IEEE OCEANS-Bergen*, pp. 1-9. IEEE, 2013.
- [RLG 2018] Román-Castro, Rodrigo, Javier López, and Stefanos Gritzalis. "Evolution and trends in IoT security." *Computer* 51, no. 7 (2018): 16-25.
- [RMB+ 2021] Resende, João S., Luís Magalhães, André Brandão, Rolando Martins, and Luís Antunes. "Towards a Modular On-Premise Approach for Data Sharing." *Sensors* 21, no. 17 (2021): 5805.
- [RMD+ 2020] Reed, Drummond, Manu Sporny, Dave Longley, Christopher Allen, Ryan Grant, Markus Sabadello, and Jonathan Holt. "Decentralized identifiers (dids) v1. 0." Draft Community Group Report (2020). Accessed November, 2021. <https://www.w3.org/TR/did-core/>
- [RN 2017] Rødseth, Ørnulf Jan, and Håvard Nordahl. "Definitions for autonomous merchant ships." In *Norwegian Forum for Unmanned Ships, Version*, vol. 1, pp. 2017-10. 2017.
- [RNH 2018] Rødseth, Ørnulf Jan, Håvard Nordahl, and Åsa Hoem. "Characterization of autonomy in merchant ships." In *2018 OCEANS-MTS/IEEE Kobe Techno-Oceans (OTO)*, pp. 1-7. IEEE, 2018.
- [RP 2018] Ribeiro, João Pires, and Ana Barbosa-Povoa. "Supply Chain Resilience: Definitions and quantitative modelling approaches—A literature review." *Computers & Industrial Engineering* 115 (2018): 109-122.
- [RR 2016] Rolls-Royce. "Remote and autonomous ship-the next steps." Page 88, 2016. Accessed November, 2021. <https://www.rolls-royce.com/~media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/aawa-whitepaper-210616.pdf>

[RRA 2019] Rubio, Juan E., Rodrigo Roman, Cristina Alcaraz, and Yan Zhang. "Tracking apts in industrial ecosystems: A proof of concept." *Journal of Computer Security* 27, no. 5 (2019): 521-546.

[RS 2017] Ranise, Silvio, and Hari Siswanto. "Automated legal compliance checking by security policy analysis." In *International Conference on Computer Safety, Reliability, and Security*, pp. 361-372. Springer, Cham, 2017.

[RSS+ 2017] Ramadan, Qusai, Mattia Salnitriy, Daniel Strüber, Jan Jürjens, and Paolo Giorgini. "From secure business process modeling to design-level security verification." In *2017 ACM/IEEE 20th International Conference on Model Driven Engineering Languages and Systems (MODELS)*, pp. 123-133. IEEE, 2017.

[RT 2014] Rødseth, Ørnulf Jan, and Åsmund Tjora. "A system architecture for an unmanned ship." In *Proceedings of the 13th international conference on computer and IT applications in the maritime industries (COMPIT)*. Verlag Schriftenreihe Schiffbau, 2014 Redworth, UK, 2014.

[RVH 2017] Ringers, Sietse, Eric Verheul, and Jaap-Henk Hoepman. "An efficient self-blindable attribute-based credential scheme." In *International Conference on Financial Cryptography and Data Security*, pp. 3-20. Springer, Cham, 2017.

[SA 2018] Scacchi, Walt, and Thomas A. Alspaugh. "Securing software ecosystem architectures: Challenges and opportunities." *IEEE Software* 36, no. 3 (2018): 33-38.

[SafeyatSea 2020] Cousins S. Increased cyber-attacks during COVID-19 highlights maritime industry vulnerabilities. SafetyatSea, September 2020.

[SAM 2016] Sabaliauskaite, Giedre, Sridhar Adepu, and Aditya Mathur. "A six-step model for safety and security analysis of cyber-physical systems." In *International Conference on Critical Information Infrastructures Security*, pp. 189-200. Springer, Cham, 2016.

[Sanders 2020] Sanders, Olivier. "Efficient Redactable Signature and Application to Anonymous Credentials." In *Public Key Cryptography (2)*, pp. 628-656. 2020.

[Sandoz 2012] Sandoz, John F. *Maritime security sector reform*. US Institute of Peace, 2012.

[Sarier 2021] Sarier, Neyire Deniz. "Comments on biometric-based non-transferable credentials and their application in blockchain-based identity management." *Computers & Security* 105 (2021): 102243.

[SB 2005] Sahai, Amit, and Brent Waters. "Fuzzy identity-based encryption." In *Annual international conference on the theory and applications of cryptographic techniques*, pp. 457-473. Springer, Berlin, Heidelberg, 2005.

[SBT+ 2015] Srinivas, Sampath, Dirk Balfanz, Eric Tiffany, Alexi Czeskis, and Fido Alliance. "Universal 2nd factor (U2F) overview." *FIDO Alliance Proposed Standard 15* (2015).

[Schäfer 2018] Schäfer, Matthias. "The fourth industrial revolution: How the EU can lead it." *European View* 17, no. 1 (2018): 5-12.

[SD 2017] Sporny, Manu, and Dave Longley. "Verifiable claims data model and representations." *W3C, Cambridge, MA, USA, Tech. Rep* (2017).

[Seattle 2019] Seattle Office and Emergency Management. "7.3 Cyber Attack and disruption," in *SEATTLE HAZARD IDENTIFICATION AND VULNERABILITY ANALYSIS*, Seattle, 2019.

[SECTRONIC 2020] SECTRONIC. "Security System for Maritime Infrastructures, Ports and Coastal zones." February 2008. Accessed November, 2021. <https://cordis.europa.eu/project/id/218245/reporting>

[Sforzin 2020] Alessandro Sforzin (editor) - CyberSec4Europe. Deliverable D3.11: "Definition of Privacy by Design and Privacy Preserving Enablers." September 2020. Accessed November, 2021. <https://cybersec4europe.eu/wp-content/uploads/2021/01/D3.11-Definition-of-Privacy-by-Design-and-Privacy-Preserving-Enablers-v1.0-submitted.pdf>

[Sforzin 2021] Alessandro Sforzin (editor) - CyberSec4Europe. Deliverable D5.4: "Requirements Analysis of Demonstration Cases Phase 2." April 2021. Accessed January 2022. <https://cybersec4europe.eu/wp-content/uploads/2021/05/D5.4-Requirements-Analysis-of-Demonstration-Cases-Phase-2-v1.0-submitted.pdf>

[SFS+ 2016] Schneider, Jonas, Nils Fleischhacker, Dominique Schröder, and Michael Backes. "Efficient cryptographic password hardening services from partially oblivious commitments." In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1192-1203. 2016.

[Sherman 2020] Justin Sherman. "U.S: Strategy for Global Internet Security Needs to Better Leverage Private Sector." October 2020. Accessed November, 2021. <https://www.cfr.org/blog/us-strategy-global-internet-security-needs-better-leverage-private-sector>

[Singer 2021] Singer N. New York Times. "Why Apple and Google's Virus Alert Apps Had Limited Success." May 2021. Accessed November, 2021. <https://www.nytimes.com/2021/05/27/business/apple-google-virus-tracing-app.html> [SK 2019] Shahraeini, Mohammad, and Panayiotis Kotzanikolaou. "A Dependency Analysis Model for Resilient Wide Area Measurement Systems in Smart Grid." *IEEE Journal on Selected Areas in Communications* 38, no. 1 (2019): 156-168.

[SK 2019] Shahraeini, Mohammad, and Panayiotis Kotzanikolaou. "A dependency analysis model for resilient wide area measurement systems in smart grid." *IEEE Journal on Selected Areas in Communications* 38, no. 1 (2019): 156-168.

[Skarmeta 2019] CyberSec4Europe Deliverable D3.1 Common Framework Handbook 1 CyberSecurity 4 Europe project. Editor Antonio Skarmeta. 2019.

[SKP+ 2019] Schauer, Stefan, Eleni-Maria Kalogeraki, Spyros Papastergiou, and Christos Douligeris. "Detecting Sophisticated Attacks in Maritime Environments using Hybrid Situational Awareness." In *2019 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*, pp. 1-7. IEEE, 2019.

[SKR+ 2019] Svilicic, Boris, Junzo Kamahara, Matthew Rooks, and Yoshiji Yano. "Maritime cyber risk management: An experimental ship assessment." *The Journal of Navigation* 72, no. 5 (2019): 1108-1120.

- [SKS+ 2021] Spanaki, Konstantina, Erisa Karafili, Uthayasankar Sivarajah, Stella Despoudi, and Zahir Irani. "Artificial intelligence and food security: swarm intelligence of AgriTech drones for smart AgriFood operations." *Production Planning & Control* (2021): 1-19.
- [SLC+ 2021] Shin, Ji Sun, Shincheol Lee, Seoyun Choi, Minjae Jo, and Sung-Hoon Lee. "A New Distributed, Decentralized Privacy-Preserving ID Registration System." *IEEE Communications Magazine* 59, no. 6 (2021): 138-144.
- [SMD+ 2020] Shakhbulatov, Denisolt, Jorge Medina, Ziqian Dong, and Roberto Rojas-Cessa. "How blockchain enhances supply chain management: A survey." *IEEE Open Journal of the Computer Society* 1 (2020): 230-249.
- [SMP 2017] Sharma, Pradip Kumar, Seo Yeon Moon, and Jong Hyuk Park. "Block-VN: A distributed blockchain based vehicular network architecture in smart city." *Journal of information processing systems* 13, no. 1 (2017): 184-195.
- [SMR+ 2021] Sousa, P. R., Magalhães, L., Resende, J. S., Martins, R., & Antunes, L. (2021). Provisioning, Authentication and Secure Communications for IoT Devices on FIWARE. *Sensors*, 21(17), 5898.
- [SON 2018] Silverajan, Bilhanan, Mert Ocaak, and Benjamin Nagel. "Cybersecurity attacks and defences for unmanned smart ships." In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 15-20. IEEE, 2018.
- [Sonatype 2020] Sonatype. "2020 State of the Software Supply Chain" [https://www.sonatype.com/hubfs/Corporate/Software%20Supply%20Chain/2020/SON\\_SSSC-Report-2020\\_final\\_aug11.pdf](https://www.sonatype.com/hubfs/Corporate/Software%20Supply%20Chain/2020/SON_SSSC-Report-2020_final_aug11.pdf)
- [Sonatype 2021] Sonatype. "2021 State of the Software Supply Chain". [https://www.sonatype.com/hubfs/Q3%202021-State%20of%20the%20Software%20Supply%20Chain-Report/SSSC-Report-2021\\_0913\\_PM\\_2.pdf?hsLang=en-us](https://www.sonatype.com/hubfs/Q3%202021-State%20of%20the%20Software%20Supply%20Chain-Report/SSSC-Report-2021_0913_PM_2.pdf?hsLang=en-us)
- [SS 2013] Sutcliffe, Alistair, and Pete Sawyer. "Requirements elicitation: Towards the unknown unknowns." In *2013 21st IEEE International Requirements Engineering Conference (RE)*, pp. 92-104. IEEE, 2013.
- [SSN+ 2020] Saad, Muhammad, Jeffrey Spaulding, Laurent Njilla, Charles Kamhoua, Sachin Shetty, DaeHun Nyang, and David Mohaisen. "Exploring the attack surface of blockchain: A comprehensive survey." *IEEE Communications Surveys & Tutorials* 22, no. 3 (2020): 1977-2008.
- [SVN+2019] Shipunov, Ilya S., Konstantin S. Voevodskiy, Anatoliy P. Nyrkov, Yuri F. Katorin, and Yuri A. Gatchin. "About the problems of ensuring information security on unmanned ships." In *2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, pp. 339-343. IEEE, 2019.
- [SZA+ 2020] Seh, Adil Hussain, Mohammad Zarour, Mamdouh Alenezi, Amal Krishna Sarkar, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan. "Healthcare data breaches: Insights and implications." In *Healthcare*, vol. 8, no. 2, p. 133. Multidisciplinary Digital Publishing Institute, 2020.

[Tafazzoli 2019] Tafazzoli, Mohammadsoroush. "Maintaining the Sustainability of Critical Infrastructure." In *Infrastructure Management and Construction*. IntechOpen, 2019.

[TD 2016] Tobin, Andrew, and Drummond Reed. "The inevitable rise of self-sovereign identity." *The Sovrin Foundation* 29, no. 2016 (2016).

[TEA 2019] Tantawy, Ashraf, Abdelkarim Erradi, and Sherif Abdelwahed. "A Modified Layer of Protection Analysis for Cyber-Physical Systems Security." In *2019 4th International Conference on System Reliability and Safety (ICSRS)*, pp. 94-101. IEEE, 2019.

[Thomopoulos 2021] Thomopoulos, Stelios CA. "Risk Assessment and Automated Anomaly Detection Using a Deep Learning Architecture." In *Artificial Neural Networks and Deep Learning-Applications and Perspective*. IntechOpen, 2021.

[TJ 2019] Tam, Kimberly, and Kevin Jones. "MaCRA: a model-based framework for maritime cyber-risk assessment." *WMU Journal of Maritime Affairs* 18, no. 1 (2019): 129-163.

[TLJ+ 2018] Erik Nilsen, Torkildson, Jingyue Li, Stig Ole Johnsen, and Jon Arne Glomsrud. "Empirical studies of methods for safety and security co-analysis of autonomous boat." *Safety and Reliability-Safe Societies in a Changing World* (2018).

[TMJ 2020] Tam, Kimberly, Kemedi Moara-Nkwe, and Kevin Jones. "The use of cyber ranges in the maritime context: Assessing maritime-cyber risks, raising awareness, and providing training." *Maritime Technology and Research* 3, no. 1 (2021): Manuscript-Manuscript.

[TML 2010] Ten, Chee-Wooi, Govindarasu Manimaran, and Chen-Ching Liu. "Cybersecurity for critical infrastructures: Attack and defense modeling." *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans* 40, no. 4 (2010): 853-865.

[TMU+ 2020] Thieme, Christoph A., Ali Mosleh, Ingrid B. Utne, and Jeevith Hegde. "Incorporating software failure in risk analysis—Part 2: Risk modeling process and case study." *Reliability Engineering & System Safety* 198 (2020): 106804.

[Tobin 2016] Tobin, Andrew, and Drummond Reed. "The inevitable rise of self-sovereign identity." *The Sovrin Foundation* 29, no. 2016 (2016).

[TSR 2003] Truman, Gregory E., Kent Sandoe, and Tasha Rifkin. "An empirical study of smart card technology." *Information & Management* 40, no. 6 (2003): 591-606.

[Tucker 2020] Tucker, B. A. *Advancing Risk Management Capability Using the OCTAVE FORTE Process*. Carnegie Mellon University, 2020.

[TXZ+ 2020] Tao, Yufei, Hekang Chen, Xiaokui Xiao, Shuigeng Zhou, and Donghui Zhang. "Angel: Enhancing the utility of generalization for privacy preserving publication." *IEEE transactions on knowledge and data engineering* 21, no. 7 (2009): 1073-1087.

[UNCTAD 2006] UNCTAD. 2006 "Maritime Security: Elements of Analytical Framework for Compliance Measurement and Risk Assessment." Accessed November, 2021. [https://unctad.org/system/files/official-document/sdtetlb20054\\_en.pdf](https://unctad.org/system/files/official-document/sdtetlb20054_en.pdf)

[UNCTAD 2020] UNCTAD. 2020 "Review report of Maritime Transport." Accessed November, 2021. <https://unctad.org/webflyer/review-maritime-transport-2020>

[URS+ 2020] Utne, Ingrid Bouwer, Børge Rokseth, Asgeir J. Sørensen, and Jan Erik Vinnem. "Towards supervisory risk control of autonomous ships." *Reliability Engineering & System Safety* 196 (2020): 106757.

[UWE] University of the West of England - Data Protection Impact Assessment. "Data Protection Impact Assessment template (DOC)." Accessed November, 2021. <https://www.uwe.ac.uk/about/structure-and-governance/data-protection/data-protection-impact-assessment>.

[VAO 2021] Varfolomeev, Alexander A., Liwa H. Alfarhani, and Zahraa Ch Olewi. "Secure-Reliable Blockchain-Based Data Access Control and Data Integrity Framework in The Environment of Smart City." In *IOP Conference Series: Materials Science and Engineering*, vol. 1090, no. 1, p. 012127. IOP Publishing, 2021.

[vdVGC+ 2016] van Der Veen, Victor, Enes Göktas, Moritz Contag, Andre Pawoloski, Xi Chen, Sanjay Rawat, Herbert Bos, Thorsten Holz, Elias Athanasopoulos, and Cristiano Giuffrida. "A tough call: Mitigating advanced code-reuse attacks at the binary level." In *2016 IEEE Symposium on Security and Privacy (SP)*, pp. 934-953. IEEE, 2016.

[VIE 2021] Vielberth, M., Glas, M., Dietz, M., Karagiannis, S., Magkos, E., and G. Pernul. "A Digital Twin-Based Cyber Range for SOC Analysts". IFIP Annual Conference on Data and Applications Security and Privacy (2021): 293-311.

[VKL 2016] Verbraeck, Alexander, Shalini Kurapati, and Heide Lukosch. "Serious games for improving situational awareness in container terminals." In *Logistics and Supply Chain Innovation*, pp. 413-431. Springer, Cham, 2016.

[vLJO+ 2019] van Laere, Joeri, Björn JE Johansson, Leif Olsson, and Peter Määttä. "Mitigating Escalation of Cascading Effects of a Payment Disruption Across Other Critical Infrastructures: Lessons Learned in 15 Simulation-Games." In *International Conference on Critical Information Infrastructures Security*, pp. 110-121. Springer, Cham, 2019.

[VMA 2021] V. Vallois, A. Mehaoua and M. Amziani, "Blockchain-based Identity and Access Management in Industrial IoT Systems," 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM), 2021, pp. 623-627.

[VVO+ 2017] Vykopal, Jan, Martin Vizváry, Radek Oslejsek, Pavel Celeda, and Daniel Tovarnak. "Lessons learned from complex hands-on defence exercises in a cyber range." In *2017 IEEE Frontiers in Education Conference (FIE)*, pp. 1-8. IEEE, 2017.

[YWC 2018] Yim, Wen-Wai, Amanda J. Wheeler, Catherine Curtin, Todd H. Wagner, and Tina Hernandez-Boussard. "Secondary use of electronic medical records for clinical research: challenges and opportunities." *Convergent science physical oncology* 4, no. 1 (2018): 014001.

- [WHH 2020] Wan, Paul Kengfai, Lizhen Huang, and Halvor Holtskog. "Blockchain-enabled information sharing within a supply chain: A systematic literature review." *IEEE Access* 8 (2020): 49645-49656.
- [WLK+ 2017] Wu, Haoyan, Zhijie Li, Brian King, Zina Ben Miled, John Wassick, and Jeffrey Tazelaar. "A distributed ledger for supply chain physical distribution visibility." *Information* 8, no. 4 (2017): 137.
- [WMK 2021] Waheed, Urooj, Yusra Mansoor, and Muhammad Ahsan Khan. "BIoT-Based Smart Agriculture: Food and Crops Efficiency and Improvement in Supply Chain Cycle." *Blockchain Technology for IoT Applications* (2021): 173.
- [WNR+ 2018] Wagner, K., B. Némethi, E. Renieris, P. Lang, E. Brunet, and E. Holst. "Self-sovereign identity: A position paper on blockchain enabled identity and the road ahead." *Identity Working Group of the German Blockchain Association* ([https://jolocom.io/wp-content/uploads/2018/10/Self-sovereign-Identity\\_-\\_Blockchain-Bundesverband-2018.pdf](https://jolocom.io/wp-content/uploads/2018/10/Self-sovereign-Identity_-_Blockchain-Bundesverband-2018.pdf)) (2018).
- [WOH+ 2018] Wiengarten, Frank, George Onofrei, Paul Humphreys, and Brian Fynes. "A supply chain view on certification standards: does supply chain certification improve performance outcomes?." In *ISO 9001, ISO 14001, and New Management Standards*, pp. 193-214. Springer, Cham, 2018.
- [Wu 1998] Wu, Thomas D. "The Secure Remote Password Protocol." In *NDSS*, vol. 98, pp. 97-111. 1998.
- [XSW+ 2021] Xu, Peng, Ruijie Sun, Wei Wang, Tianyang Chen, Yubo Zheng, and Hai Jin. "SDD: A trusted display of FIDO2 transaction confirmation without trusted execution environment." *Future Generation Computer Systems* 125 (2021): 32-40.
- [YCG 2019] Yang, Li, Xiedong Cao, and Xinyu Geng. "A novel intelligent assessment method for SCADA information security risk based on causality analysis." *Cluster Computing* 22, no. 3 (2019): 5491-5503.
- [YI 2019] Yeboah-Ofori, Abel, and Shareeful Islam. "Cyber security threat modeling for supply chain organizational environments." *Future Internet* 11, no. 3 (2019): 63.
- [YZC+ 2020] Yu, Miao, Jianwei Zhuge, Ming Cao, Zhiwei Shi, and Lin Jiang. "A survey of security vulnerability analysis, discovery, detection, and mitigation on IoT devices." *Future Internet* 12, no. 2 (2020): 27.
- [ZB 2012] Zhu, Quanyan, and Tamer Başar. "A dynamic game-theoretic approach to resilient control system design for cascading failures." In *Proceedings of the 1st international conference on High Confidence Networked Systems*, pp. 41-46. 2012.
- [ZFG 2014] Zhu, Bo, Xinxin Fan, and Guang Gong. "Loxin—A solution to password-less universal login." In *2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 488-493. IEEE, 2014.
- [ZKS+ 2021] Zhang, Zhiyi, et al. EL PASSO: Efficient and Lightweight Privacy-preserving Single Sign On. *Proc. Priv. Enhancing Technol.*, 2021, vol. 2021, no 2, p. 70-87.

---

[ZLA+ 2021] Zhihan Lv, Liang Qiao, Amit Kumar Singh, Qingjun Wang, “AI-empowered IoT Security for Smart Cities”, ACM Transactions on Internet Technology, volume 2, issue 4, pp: 1–21, <https://doi.org/10.1145/3406115>, November 2021

[ZLL+ 2021] Zhihao Yu, Liang Song, Linhua Jiang, Omid Khold Sharafi, “Systematic literature review on the security challenges of blockchain in IoT-based smart cities”, Kybernetes, <https://doi.org/10.1108/K-07-2020-0449>

[ZPK+ 2019] Artur Zolich; David Palma; Kimmo Kansanen; Kay Fjørtoft; Joao Sousa; Karl H. Johansson; Yuming Jiang; Hefeng Dong; Tor A. Johansen, "Survey on Communication and Networks for Autonomous Marine Systems." *Journal of Intelligent & Robotic Systems* (2019) 95:789–813

[ZTB+ 2016] Zickau, Sebastian, Dirk Thatmann, Artjom Butyrtschik, Iwailo Denisow, and Axel Küpper. "Applied attribute-based encryption schemes." In 19th International ICIN Conference-Innovations in Clouds, Internet and Networks, pp. 88-95. 2016.