



Cyber Security for Europe



D4.4

Research and Development Roadmap 2

Document Identification	
Due date	31 January 2021
Submission date	29 January 2021
Revision	3.0

Related WP	WP4	Dissemination Level	Public
Lead Participant	FORTH	Lead Author	Evangelos Markatos (FORTH)
Contributing Beneficiaries	AIT, Atos, 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

Abstract:

This is the second 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 (12 months), medium term (until the end of the project), and long term (beyond the end of the project). To emphasize the European nature of these roadmaps, each vertical clearly demonstrates how it can contribute to dimensions with significant European impact including European **Digital Sovereignty**, the **COVID-19** pandemic, and the **European Green Deal**. Finally, a SWOT (Strengths, Weaknesses, Opportunities and Threats) Analysis clearly demonstrates how Europe can approach the research in each area, what are the hurdles in the way, what are the strengths that can be exploited, and what can be expected at the end.

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. 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 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 document, the second 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 a *SWOT analysis* that builds on strengths and addresses shortcomings:
 - what are the strengths of Europe in these verticals?
 - what are the weaknesses?
 - what (global) opportunities may exist?
 - what threats should we be careful of?
3. explaining how the chosen research priorities interact with the *important dimensions* of European policies in 2020-2021 as they relate to:
 - the **European Digital Sovereignty**,
 - the new reality imposed by **COVID-19**, and
 - the **Green Deal**.

How to read this document

To provide a uniform approach to the roadmap, each vertical is covered in one section starting from section 3 all the way to section 9. In the interests of homogeneity, subsections are structured as follows:

- Subsections¹ *.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 the research challenges and provide background information. More specifically:
 - Subsections *.5.1 describe the state of the art for each vertical and subsections *.5.2 indicate the final goal;
 - Subsections *.5.3 provide a SWOT analysis;
 - Subsections *.5.4 explain how each vertical contributes to **European Digital Sovereignty**;
 - Subsections *.5.5 describe the interactions with **COVID-19**;
 - Subsections *.5.6 describe the interactions with the **Green Deal**; and
 - The remaining subsections of *.5 describe the research challenges.

¹ When we write *.1 we mean subsections 3.1, 4.1, 5.1 etc. until subsection 9.1. When we write *.2 we mean subsections 3.2, 4.2, 5.2, ... 9.2, and so on and so forth.

- Subsections *.6 describe the mapping of the challenges to the big picture.
- Subsections *.7 describe the methods and tools for the research challenges.
- Subsections *.8 provide the **roadmap** for each vertical. Each roadmap is structured in three phases:
 - Short-term,
 - Medium-term, and
 - Long-term,
- Finally, subsections *.9 provide a **summary** of each vertical.

To place this work in context, Section 10 provides progress with respect to work reported in the first Roadmap (D4.3 [Markatos 2020]). Finally, section 11 surveys roadmaps (or similar research priorities documents) that were published in 2020 including **ENISA**²'s annual cybersecurity prioritisation document [ENISA 2020B], **Europol**'s annual publication IOCTA (Internet Organized Threat Assessment), which lists the evolution of the threats in cybercrime [EUROPOL 2020], **JRC**³'s Digital Anchor, **SPARTA**'s Roadmap, etc.

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.

² ENISA is the European Network and Information Security Agency

³ JRC is the Joint Research Centre (of the European Commission)

Document information

Contributors

Name	Partner
Cristina Alcaraz	UMA
Ahmad Amro	NTNU
Marco Angelini	ENG
Elias Athanasopoulos	UCY
Jorge Bernal	UMU
Karin Bernsmed	SINTEF
Panagiotis Bountakas	UPRC
Vanesa Gil Laredo	BBVA
Laura Colombini	ISGS
Said Daoudagh	CNR
Jérémy Decis	DAWEX
Christos Douligeris	UPRC
Carmen Fernández Gago	UMA
Jesús García	UMU
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 Pääjänen	JAMK
Spyros Papastergiou	UPRC
Ivan Pashchenko	UNITN
Juan Carlos Pérez Bañ	Atos
Salvador Perez	UMU
Rodrigo Roman	UMA
Michael Salmony	TDL
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 Rannenber	GUF
Ahad Niknia	GUF

History

Version	Date	Authors	Comment
0.01	October 10 th 2020	Evangelos Markatos	Table of Contents
0.02	October 22 th 2020	Rafael Torres and Jesus García	Section 5
0.03	October 22 th 2020	Alba Hita and Salvador Perez	Section 9
0.04	November 4 th 2020	Marko Kompara	Section 5
0.05	November 4 th 2020	Stephan Krenn	Section 5
1.0	December 16 th 2020	Evangelos Markatos (based on input from all partners)	First version for high-level review
2.0	January 15 th 2021	Evangelos Markatos (based on input from all partners)	Second version addresses the comments of the reviewers
3.0	January 28 th 2021	Evangelos Markatos	Third version addresses the comments of the PC

Short Table of Contents:

Executive Summary	iii
1 Introduction.....	1
2 Context and Methodology	3
3 Open Banking	11
4 Supply Chain Security Assurance.....	61
5 Privacy-Preserving Identity Management	98
6 Incident Reporting	126
7 Maritime Transport.....	157
8 Medical Data Exchange	200
9 Smart Cities.....	230
10 Progress since D4.3.....	280
11 Related Work.....	285
12 Summary	297
13 References.....	298

Long Table of Contents:

Executive Summary	iii
How to read this document	iii
1 Introduction.....	1
1.1 Connections with Deliverable D4.3 (Roadmap 1)	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	4
2.1.2 What is at stake?.....	6
2.1.3 Who are the attackers?	6
2.1.4 What can be done about it?	7
2.2 Summary of CyberSec4Europe Demonstration Cases.....	7
2.2.1 Open Banking.....	7
2.2.2 Supply Chain Security Assurance.....	8
2.2.3 Privacy-preserving identity management.....	8
2.2.4 Incident Reporting.....	8
2.2.5 Maritime Transport	9
2.2.6 Medical Data Exchange	9
2.2.7 Smart Cities.....	10
3 Open Banking	11
3.1 The Big Picture	11
3.1.1 RTS SCA.....	12
3.1.2 PSD2 and GDPR	13
3.1.3 European Data Strategy.....	14
3.1.4 Summary	15
3.2 Overview	15
3.3 What is at stake?.....	16
3.3.1 What needs to be protected?	17
3.3.2 What could go wrong?	17
3.3.3 Social Engineering & Malware Attacks.....	17
3.3.4 Certificate Verification.....	18

3.3.5	GDPR & PSD2.....	18
3.3.6	APIs.....	19
3.3.7	Bank Administration.....	20
3.3.8	Circles of Trust.....	20
3.3.9	What is the worst thing that can happen?.....	21
3.4	Who are the attackers?.....	22
3.5	Research Challenges.....	23
3.5.1	State of the Art.....	23
3.5.1.1	Summary.....	23
3.5.1.2	The Bad News.....	24
3.5.1.3	The Good News.....	29
3.5.2	Final Goal.....	34
3.5.3	SWOT Analysis.....	34
3.5.3.1	Strengths.....	35
3.5.3.2	Weaknesses.....	36
3.5.3.3	Opportunities.....	36
3.5.3.4	Threats.....	37
3.5.4	European Digital Sovereignty.....	38
3.5.5	COVID-19 Dimension.....	41
3.5.5.1	Opportunities.....	41
3.5.5.2	Threats.....	42
3.5.6	Green Deal Dimension.....	43
3.5.7	Brexit Dimension.....	44
3.5.8	Sector-specific Dimensions.....	45
3.5.8.1	The United States.....	45
3.5.8.2	Asia.....	46
3.5.9	Challenge 1: Mapping of stakeholder interaction in end-to-end Open Banking processing.....	48
3.5.10	Challenge 2: Setting up and discontinuing business relationships.....	49
3.5.11	Challenge 3: Cross-border cooperation under differing legislation and security controls... ..	49
3.5.12	Challenge 4: Convenient and Compliant Authentication.....	51
3.5.13	Challenge 5: Real time Revocation of Right of Access.....	52
3.5.14	Challenge 6: Corporate Open Banking Security.....	52

3.6	Mapping of the Challenges to the Big Picture	53
3.7	Methods, Mechanisms, and Tools.....	54
3.7.1	Challenge 1: Mapping of stakeholder interaction in end-to-end Open Banking processing 54	
3.7.2	Challenge 2: Setting up and discontinuing business relationships.....	55
3.7.3	Challenge 3: Cross-border cooperation under differing legislation and security controls...	55
3.7.4	Challenge 4: Convenient and compliant authentication.....	56
3.7.5	Challenge 5: Real time revocation of right of access.....	56
3.7.6	Challenge 6: Corporate open banking security	57
3.8	Roadmap	59
3.8.1	12-month plan	59
3.8.2	2-year (or until the end of the project) plan	59
3.8.3	Beyond the end of the project	59
3.9	Summary	60
4	Supply Chain Security Assurance.....	61
4.1	The Big Picture	61
4.2	Overview	61
4.3	What is at stake?.....	62
4.3.1	What needs to be protected?	62
4.3.2	What is expected to go wrong?	63
4.3.3	What is the worst thing that can happen?.....	65
4.4	Who are the attackers?	66
4.5	Research Challenges	67
4.5.1	State of the Art.....	67
4.5.1.1	Supply chain risks, vulnerabilities and resilience	67
4.5.1.2	Attack prevention, detection and response in supply chains.....	69
4.5.1.3	Data sharing in supply chain ecosystems.....	71
4.5.1.4	Monitoring for compliance	74
4.5.2	Final Goal.....	76
4.5.3	SWOT Analysis	77
4.5.3.1	Strengths.....	78
4.5.3.2	Weaknesses	78
4.5.3.3	Opportunities.....	79
4.5.3.4	Threats.....	80

4.5.4	European Digital Sovereignty	80
4.5.5	COVID-19 Dimension	81
4.5.6	Green Dimension	83
4.5.7	Sector-specific Dimensions.....	84
4.5.8	Challenge 1: Detection and management of supply chain security risks.....	84
4.5.9	Challenge 2: Security hardening of supply chain infrastructures, including cyber and physical systems	85
4.5.10	Challenge 3: Security and privacy of supply chain information assets and goods	87
4.5.11	Challenge 4: Management of the certification of supply partners	89
4.6	Mapping of the Challenges to the Big Picture	90
4.7	Methods, Mechanisms, and Tools.....	91
4.7.1	Challenge 1: Risk management methodologies and frameworks	91
4.7.2	Challenge 2: Distributed detection, continuous monitoring and incident management	92
4.7.3	Challenge 3: Traceability, Shared Data Spaces	93
4.7.4	Challenge 4: Continuous Certification.....	94
4.8	Roadmap	95
4.8.1	12-month plan	95
4.8.2	2-year (or until the end of the project) plan	95
4.8.3	Beyond the end of the project plan	96
4.9	Summary	97
5	Privacy-Preserving Identity Management	98
5.1	The Big Picture	98
5.2	Overview	98
5.3	What is at stake?.....	100
5.3.1	What needs to be protected?	100
5.3.2	What is expected to go wrong?	100
5.3.3	What is the worst thing that can happen?.....	101
5.4	Who are the attackers?	102
5.5	Research Challenges	103
5.5.1	State of the Art	103
5.5.1.1	System-based credential hardening.....	103
5.5.1.2	Unlinkability and minimal disclosure	104
5.5.1.3	Distributed oblivious identity management	104

5.5.1.4	Privacy preservation in blockchain	105
5.5.1.5	Password-less authentication	105
5.5.1.6	GDPR and eIDAS impact interoperability.....	106
5.5.1.7	Identity Management Solutions for the IoT	107
5.5.2	Final Goal.....	108
5.5.3	SWOT Analysis	108
5.5.3.1	Strengths.....	109
5.5.3.2	Weaknesses	109
5.5.3.3	Opportunities.....	110
5.5.3.4	Threats.....	110
5.5.4	European Digital Sovereignty	110
5.5.5	COVID-19 Dimension	111
5.5.6	Green Dimension	112
5.5.7	Sector-specific Dimensions.....	112
5.5.8	Challenge 1: System-based credential hardening	112
5.5.9	Challenge 2: Unlinkability and minimal disclosure.....	113
5.5.10	Challenge 3: Distributed oblivious identity management.....	113
5.5.11	Challenge 4: Privacy preservation in blockchain.....	115
5.5.12	Challenge 5: Password-less authentication	116
5.5.13	Challenge 6: GDPR and eIDAS impact on Identity Management.....	117
5.5.14	Challenge 7: Identity Management Solutions for the IoT.....	119
5.6	Mapping of the Challenges to the Big Picture	119
5.7	Methods, Mechanisms, and Tools.....	120
5.7.1	System-based credential hardening.....	120
5.7.2	Unlinkability and minimal disclosure	120
5.7.3	Distributed oblivious identity management	121
5.7.4	Privacy preservation in blockchain	121
5.7.5	Password-less authentication	121
5.7.6	GDPR guidelines and eIDAS interoperability	121
5.7.7	Identity Management Solutions for the IoT	121
5.8	Roadmap	122
5.8.1	12-month plan	122
5.8.2	2-year (or until the end of the project) plan	123
5.8.3	Beyond the end of the project plan	124

5.9	Summary	124
6	Incident Reporting	126
6.1	The Big Picture	126
6.2	Overview	126
6.3	What is at stake?.....	127
6.3.1	What is the underlying need?.....	127
6.3.2	What is expected to go wrong?	130
6.3.3	What is the worst thing that can happen?.....	132
6.4	Who are the main stakeholders?	133
6.5	Research Challenges	135
6.5.1	State of the Art	136
6.5.1.1	Security Incident Reporting	136
6.5.1.2	Risk assessment methodologies on incident reports	138
6.5.2	Final Goal.....	139
6.5.3	SWOT Analysis	140
6.5.3.1	Strengths.....	140
6.5.3.2	Strengths.....	140
6.5.3.3	Weaknesses	141
6.5.3.4	Opportunities.....	142
6.5.3.5	Threats.....	143
6.5.4	European Digital Sovereignty	144
6.5.5	COVID-19 Dimension	144
6.5.6	Green Dimension	146
6.5.7	Sector-specific Dimensions.....	146
6.5.8	Challenge 1: Lack of harmonization of procedures	147
6.5.9	Challenge 2: Facilitate the collection and reporting of incident and/or data leaks	148
6.5.10	Challenge 3: Promote a collaborative approach for sharing incident reports to increase risk quantification, mitigation and thus overall cyber resilience	149
6.6	Mapping of the Challenges to the Big Picture	150
6.7	Methods, Mechanisms, and Tools.....	150
6.7.1	Incident Data Collection	150
6.7.2	Incident Impact Assessment (and transferability to other organization)	151
6.7.3	Incident Reporting.....	151

6.7.4	Collaborative incident sharing platform.....	152
6.8	Roadmap	153
6.8.1	12-month plan	153
6.8.2	3-year (or until the end of the project) plan	153
6.8.3	Beyond the end of the project plan	154
6.9	Summary	155
7	Maritime Transport.....	157
7.1	The Big Picture	157
7.2	Overview	158
7.3	What is at stake?.....	159
7.3.1	What needs to be protected?	159
7.3.2	What is expected to go wrong?.....	162
7.3.3	What is the worst thing that can happen?.....	163
7.4	Who are the attackers?.....	163
7.4.1	Maritime Threat Agents	163
7.4.1.1	Agent: Activists.....	163
7.4.1.2	Agent: Competitor.....	163
7.4.1.3	Agent: Corrupt Government Official	164
7.4.1.4	Agent: Cyber Vandal.....	164
7.4.1.5	Agent: Data Miner/Thief.....	164
7.4.1.6	Agent: Employee, Disgruntled.....	164
7.4.1.7	Agent: Government Spy.....	164
7.4.1.8	Agent: Government Cyberwarrior	164
7.4.1.9	Agent: Internal Spy	164
7.4.1.10	Agent: Sensationalist/Irrational Individual	165
7.4.1.11	Agent: Terrorist.....	165
7.4.1.12	Agent: Mobster.....	165
7.4.1.13	Agent: Mobster.....	165
7.4.1.14	Agent: Mobster.....	165
7.4.1.15	Agent: Mobster.....	165
7.5	Research Challenges	166
7.5.1	State of the Art	166
7.5.1.1	Legal and regulatory background.....	166
7.5.1.2	Risk assessment in the maritime transport sector	168

7.5.1.3	Security hardening for critical (maritime) systems	170
7.5.1.4	Maritime communication system security and trust infrastructures	173
7.5.1.5	Secure autonomous ships	176
7.5.1.6	Resilience in critical (maritime) infrastructures.....	177
7.5.2	Final Goal.....	178
7.5.3	SWOT Analysis	179
7.5.3.1	Strengths.....	179
7.5.3.2	Weaknesses	180
7.5.3.3	Opportunities.....	180
7.5.3.4	Threats.....	181
7.5.4	European Digital Sovereignty	181
7.5.5	COVID-19 Dimension	182
7.5.6	Green Dimension	183
7.5.7	Sector-specific Dimensions.....	183
7.5.8	Identified Research Challenges in the Maritime Transport Sector	184
7.5.8.1	Challenge 1: Early identification and assessment of risks, threats and attack paths for critical maritime systems.....	184
7.5.8.2	Challenge 2: Security hardening of maritime infrastructures, including cyber and physical systems	185
7.5.8.3	Challenge 3: Resilience of critical maritime systems	186
7.5.8.4	Challenge 4: Maritime system communication security.....	187
7.5.8.5	Challenge 5: Securing autonomous ships	188
7.6	Mapping of the Challenges to the Big Picture	190
7.7	Methods, Mechanisms, and Tools.....	191
7.7.1	Risk management and threat modelling methodologies for the Maritime Transport sector	191
7.7.2	Secure Autonomous Ships	191
7.7.3	Attack scenarios/simulation - security hardening	192
7.7.4	Secure Maritime Communications.....	193
7.7.5	Resilience	193
7.8	Roadmap	195
7.8.1	12-month plan	195
7.8.2	2-year (or until the end of the project) plan	196

7.8.3	Beyond the end of the project plan	197
7.9	Summary	197
8	Medical Data Exchange	200
8.1	The Big Picture	200
8.2	Overview	200
8.3	What is at stake?.....	201
8.3.1	What needs to be protected?	201
8.3.2	What is expected to go wrong?.....	202
8.3.3	What is the worst thing that can happen?.....	203
8.4	Who are the attackers?	203
8.5	Research Challenges	204
8.5.1	State of the Art	204
8.5.1.1	Identity management and eIDs.....	205
8.5.1.2	Medical data privacy	206
8.5.1.3	Legal and regulatory considerations	209
8.5.2	Final Goal.....	210
8.5.3	SWOT Analysis	210
8.5.3.1	Strengths.....	211
8.5.3.2	Weaknesses	212
8.5.3.3	Opportunities.....	212
8.5.3.4	Threats.....	212
8.5.4	European Digital Sovereignty	212
8.5.5	COVID-19 Dimension	214
8.5.5.1	Medical Data Exchange demonstrator facing Covid-19.....	214
8.5.5.2	Mobile contact tracing apps in Europe.....	215
8.5.6	Sector-specific Dimensions.....	219
8.5.7	Challenge 1: Security and privacy	219
8.5.8	Challenge 2: Mechanisms for preserving user data privacy	220
8.5.9	Challenge 3: Trustworthiness on the data exchange platform	220
8.5.10	Challenge 4: Accomplish regulation during the data sharing process	221
8.5.11	Challenge 5: Data exchange platform user experience	223
8.6	Mapping of the Challenges to the Big Picture	223
8.7	Methods, Mechanisms, and Tools.....	223
8.7.1	Challenge 1: Security tools	224

8.7.2	Challenge 2: Privacy-preserving assets.....	224
8.7.3	Challenge 3: Trust mechanisms	225
8.7.4	Challenge 4: Regulation accomplish.....	225
8.7.5	Challenge 5: User Experience	225
8.8	Roadmap	226
8.8.1	12-month plan	226
8.8.2	2-year (or until the end of the project) plan	227
8.8.3	Beyond the end of the project plan	228
8.9	Summary	228
9	Smart Cities.....	230
9.1	The Big Picture	230
9.2	Overview	231
9.3	What is at stake?.....	232
9.3.1	What needs to be protected?	232
9.3.2	What is expected to go wrong?	235
9.3.3	What is the worst thing that can happen?.....	238
9.4	Who are the attackers?	240
9.5	Research Challenges	241
9.5.1	State of the Art	241
9.5.1.1	Secure Data Sharing.....	241
9.5.1.2	Cyber Risk Assessment.....	243
9.5.1.3	Social Engineering and Phishing	246
9.5.2	Final Goal.....	248
9.5.3	SWOT Analysis	248
9.5.3.1	Strengths.....	249
9.5.3.2	Weaknesses	250
9.5.3.3	Opportunities.....	250
9.5.3.4	Threats.....	250
9.5.3.5	European Digital Sovereignty	250
9.5.4	COVID-19 Dimension	251
9.5.5	Green Dimension	252
9.5.6	Challenge 1: Trusted Digital Platform	252

9.5.7	Challenge 2: Cyber threat intelligence and analysis platform	253
9.5.8	Challenge 3: Cyber competence and awareness program.....	255
9.5.9	Challenge 4: Privacy by design.....	256
9.5.10	Challenge 5: Cyber response and resilience.....	258
9.5.11	Challenge 6: End user trusted data management	259
9.5.12	Challenge 7: Interoperability between legacy and new systems.....	261
9.5.13	Challenge 8: Cyber fault/failure detection and prevention	262
9.5.14	Challenge 9: Logging and monitoring	264
9.5.15	Challenge 10: Information security and operational security	266
9.6	Mapping of the Challenges to the Big Picture	268
9.7	Methods, Mechanisms, and Tools.....	269
9.7.1	Integrated Security Risk Framework	270
9.7.2	Cyber competences and awareness program.....	272
9.7.3	Privacy by design and end user trusted data management.....	273
9.8	Roadmap	274
9.8.1	12-month plan	275
9.8.2	2-year (or until the end of the project) plan	276
9.8.3	Beyond the end of the project plan	277
9.9	Summary	278
10	Progress since D4.3.....	280
10.1	Open Banking.....	280
10.2	Supply Chain Security Assurance.....	280
10.3	Privacy-preserving identity management.....	281
10.4	Incident Reporting.....	282
10.5	Maritime Transport	282
10.6	Medical Data Exchange	283
10.7	Smart Cities.....	283
11	Related Work.....	285
11.1	JRC: Digital Anchor.....	285
11.2	Internet Organised Crime Threat Assessment (IOCTA) 2020.....	286
11.3	Strategic Foresight Report 2020.....	286
11.4	Cyberwatching.eu EU Cybersecurity & Privacy Interim Roadmap	287
11.5	SPARTA Roadmap	288
11.6	ENISA Report on AI Cybersecurity Challenges.....	288

11.7	ENISA Threat Landscape 2020	289
11.7.1	Overview	289
11.7.2	What has changed?.....	290
11.7.3	Recommendations.....	290
11.7.4	Top 15 Threats	290
12	Summary.....	297
13	References.....	298

List of Figures

Figure 1: Open Banking will change the way financial transactions are being carried out.....	7
Figure 2: Collecting and re-using medical data is expected to result in breakthroughs in medicine.....	9
Figure 3: Account Information Service Provider.....	12
Figure 4: Payment Initiation Service Provider (PISP).....	12
Figure 5: Overview of elements of API scheme	32
Figure 6: Open Banking SWOT Summary	35
Figure 7: Supply Chain SWOT Summary	77
Figure 8: Privacy-Preserving Identity Management SWOT Summary	109
Figure 9: Graphical overview of the NIS Directive. Source: Incident notification for DSPs in the context of the NIS Directive.....	129
Figure 10: Incident Reporting SWOT Summary	140
Figure 11: The big picture of a resilient EU maritime transport ecosystem.....	158
Figure 12: The ENISA taxonomy for critical maritime assets (Source: [ENISA 2019])	160
Figure 13: Context diagram for autonomous ship operation (Source: [RN 2017])	161
Figure 14: The ENISA threat taxonomy for the maritime transport sector (Source: [ENISA 2019])	162
Figure 15. Examples of maritime communication channels.....	174
Figure 16: Overview of the APS Context	175
Figure 17: On-board network architecture.....	175
Figure 18: Maritime Transport SWOT Summary.....	179
Figure 19: Medical Data Exchange SWOT	211
Figure 20: Stakeholders and services.....	231
Figure 21: IoT Assembly Taxonomy (Source [ENISA 2018]).....	234
Figure 22: Industry 4.0 Asset Taxonomy (Source: [ENISA 2018])	235
Figure 23: IoT Threat Taxonomy (Source: [ENISA 2018])	237
Figure 24: IoT Threats Impact	239
Figure 25: Intel Threats Identification	241
Figure 26: Smart Cities SWOT Summary	249
Figure 27: PDCA cycles for SC vertical.....	271

List of Tables

Table 1: Open Banking global comparisons	38
Table 2: Challenges identified in the Open Banking vertical and tools needed to address them	57
Table 3: Challenges identified in the Supply Chain Vertical and Tools needed to address them	94
Table 4: Challenges identified in the Privacy-Preserving Identity Management Vertical and Tools needed to address them.....	122
Table 5: Challenges identified in the Incident Reporting Vertical and Tools needed to address them	152
Table 6: Challenges identified in the Maritime Transport Vertical and Tools needed to address them....	193
Table 7: Interoperability of mobile contact tracing apps in some EU Member States	215
Table 8: Interoperability of mobile contact tracing apps in some EU Member States	216
Table 9: Challenges identified in the Medical Data Exchange Vertical and Tools needed to address them	226
Table 10: Challenges identified in the Smart Cities Vertical and Tools needed to address them.	269
Table 11: Top 15 threats identified by ENISA	290

List of Acronyms and Abbreviations

<i>A</i>	ABC	Attribute-Based Credentials
	AISP	Account Information Service Provider
	API	Application Program Interface
	ASLR	Address Space Layout Randomization
	ASC	Autonomous Ship Controller
	ASPSP	Account Servicing Payment Service Provider
<i>C</i>	CC0	Creative Commons No Rights Reserved Licence
	CERT	Cyber Emergency Response Team
	CE-S	Cyber Enabled Ships
	CII	Critical Information Infrastructure
	CNIL	Commission Nationale de l'informatique et des Libertés
	CPS	Cyber Physical Systems
	CS4E	CyberSec4Europe
	CTI	Cyber Threat Intelligence
	CYSM	Cyber/Physical Security Management Systems
	<i>D</i>	DEP
DLT		Distributed Ledger Technology
DPIA		Data Privacy Impact Assessment
<i>E</i>	EBA	European Banking Authority
	ECISO	European CyberSecurity Organisation
	EDPB	European Data Protection Board
	EDPS	European Data Protection Supervisor
	EEA	European Economic Area
	eID	electronic IDentity
	eIDAS	electronic IDentification, Authentication and trust Services
	ENISA	European Network and Information Security Agency
<i>F</i>	FIDO	Fast IDentity Online Alliance
<i>G</i>	GDPR	General Data Protection Regulation
	GAFAM	Google, Amazon, Facebook, Apple and Microsoft
	GNSS	Global Navigation Satellite System
<i>I</i>	IBAN	International Bank Account Number
	IaaS	Infrastructure as a Service
	ICS	Industrial Control Systems
	ICT	Information and Communication Technologies
	IDM	Identity Management
	IoT	Internet of Things
	IIoT	Industrial Internet of Things
	IMO	International Maritime Organization

	ISO	International Organization for Standardization
	ITU	International Telecommunication Union
<i>J</i>	JRC	Joint Research Centre (of the European Commission)
<i>L</i>	LPA	Local Public Administration
<i>M</i>	MARISA	Maritime Integrated Surveillance Awareness
	MEDUSA	Multi-ordEr Dependency approaches for managing cascading effects in port's global sUpply chain and their integration in riSk Assessment frameworks
	MITIGATE	Multidimensional, IntegraTed, rIsk assessment framework and dynamic, collaborative risk manaGement tools for critical information infrAstrucTrurEs
	MSRAM	Maritime Security RiskAnalysis Model
<i>N</i>	NIS	Network and Information Security
	NIST	National Institute of Standards and Technology
<i>O</i>	OSINT	Open Source Intelligence
	OT	Operational Technologies
<i>P</i>	PA	Public Administration
	PET	Privacy Enhancing Technologies
	PHA	Preliminary Hazard Analysis
	PISP	Payment Initiation Services Provider
	PKI	Public Key Infrastructure
	PSD2	Payment Services Directive 2
	PSP	Payment Services Provider
	PSU	Payment Services User
	PUF	Physical/physically Unclonable Function
<i>R</i>	RTK	Real-Time Kinematic
	RTS	Regulatory Technical Standards
	RTU	Remote Terminal Unit
	RFID	Radio-Frequency IDentification
<i>S</i>	SaaS	Software as a Service
	SAML	Security Assertion Markup Language
	SC	Smart City
	SCA	Strong Customer Authentication
	SCRM	Supply Chain Risk Management
	SIEM	Security Information and Event Management
	SME	Small or Medium-sized Enterprise
	SSM	Six-Step-Model
	SWOT	Strengths, Weaknesses, Opportunities and Threats
<i>T</i>	TPP	Third Party Provider
<i>U</i>	UAV	Unnamed Aerial Vehicles

V	VDES	VHF Data Exchange System
W	WLAN	Wireless Local Area Network

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 cybersecurity prioritisation document [ENISA 2020B], **ENISA** presents the threats, attacks, as well as the important research topics in the area of cybersecurity. **Europol** also recently published the 2020 edition of its annual publication IOCTA (Internet Organized Threat Assessment), in which it lists the evolution of the threats in cybercrime [EUROPOL 2020].

In the context of the CyberSec4Europe project, we also publish a yearly research and development roadmap. Unlike 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 D4.4), which is the second in the series, focuses

- (i) on *updating* the research priorities,
- (ii) on providing a *SWOT analysis*, and
- (iii) on explaining how the chosen research priorities interact with the important dimensions of European policies in 2020 as they relate to:
 - a. *European Digital Sovereignty*,
 - b. *COVID-19*, and
 - c. the *Green Dimension*.

The rest of this document is structured as follows: Section 0 presents the methodology followed. 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 first roadmap, and section 11 presents related work: roadmaps and similar documents that have been published in 2020.⁴ Such documents include ENISA’s Threat Landscape, Europol’s IOCTA, JRC’s Digital Anchor, SPARTA’s Roadmap, etc.

VERTICAL AREAS

OPEN BANKING

SUPPLY-CHAIN SECURITY
ASSURANCE

PRIVACY-PRESERVING
IDENTITY MANAGEMENT

INCIDENT REPORTING

MARITIME TRANSPORT

MEDICAL DATA EXCHANGE

SMART CITIES

⁴ Note that Roadmaps published before 2020 were included in the related work of Deliverable D4.3

1.1 Connections with Deliverable D4.3 (Roadmap 1)

The project's second roadmap, as implemented in the current deliverable, D4.4, is carefully designed to be self-contained. Otherwise, this second roadmap, which is a natural progression of the 1st roadmap (D4.3 delivered in 2020), would be hard to read. To assist in reading and in parallel stress this natural progression between the two roadmaps, we have formatted the content of the first roadmap in a lightly shaded background. Therefore, readers familiar with deliverable D4.3 (the first roadmap) can easily skip the shaded sections, or use them as a back reference, while studying the new material.

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**?
- What are the **research challenges** in this area?
 - **State of the Art**
 - What has been done?
 - **Final Goal**
 - Where do we want to go? That is, if we do the research in this area, what do we expect to happen?
 - **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**
 - What is the interaction of this area with COVID-19?
 - **Green Dimension**
 - What is the interaction of this area with the green dimension? Is there any contribution that can be made?
 - Sector-specific dimensions
 - Is there interaction with any sector-specific dimensions?
- 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:

2.1.1.1 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. In a future roadmap, we will reassess the important dimensions.

- **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 (including CyberSec4Europe) explore the steps that need to be taken in order to restore European Sovereignty in cyberspace.⁵ Against this background, support has been growing for a new policy approach designed to enhance Europe's strategic autonomy in the digital field.⁶ In this setting we would like to understand:
 - How does each vertical contribute to achieving European Digital Sovereignty?
 - How does the goal of European Digital Sovereignty impact the research that needs to be done in each vertical?
- **COVID-19**
 - Over the past year we have witnessed probably the largest pandemic in living memory for most of us. This pandemic had (and at the time of writing is still having) a profound impact on the way we work, study and entertain ourselves. Because of the pandemic, several activities (such as schooling) moved completely or partially online. In this section we would like to explore what kind of interaction there exists between each vertical and the pandemic. For example, for data sharing in the context of Smart Cities or in the context of the medical field, what is its interaction with COVID-19? e.g.,
 - What kind of research needs to be done in this vertical to address the impact of COVID-19?
 - How has the onset of the pandemic impacted the research activities that need to be performed in this vertical?
- **The Green Deal Dimension**
 - It is widely acknowledged that climate change and environmental degradation are an existential threat to Europe and the world.⁷ 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. We believe that several of the verticals have significant interactions with the European Green Deal. In this section we would like to explore:
 - How can research in the area of the vertical contribute to the Green Deal?
 - How do climate change and environmental degradation impact the vertical and the research being done for it?

All in all, we would like to understand and report how the cybersecurity research challenges may contribute to the improvement of these dimensions and under what circumstances.

⁵ <https://cybersec4europe.eu/convergence/roadmapping-focus-group/>

⁶ [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)

⁷ https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_en

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 companies⁸. 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.

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

⁸ <https://www.cnn.com/2019/07/30/five-of-the-biggest-data-breaches-ever.html>

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 out⁹

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.

⁹ image distributed under Creative Commons CC0 courtesy of <https://www.pxfuel.com/en/free-photo-osvpk>

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.

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 medicine¹⁰

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.

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

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 GDPR¹¹ (General Data Protection Regulation), NIS¹² Directive¹³, 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 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.

¹¹ <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

¹² NIS stands for Network and Information Security

¹³ <https://eur-lex.europa.eu/eli/dir/2016/1148/oj>

3 Open Banking

3.1 The Big Picture

The revised Payment Services Directive (PSD2)¹⁴ updates and enhances the EU rules put in place by the initial PSD adopted in 2007¹⁵. PSD2 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.

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 ASPSPs¹⁶ can rely on dedicated interfaces (APIs), that should be properly configured to reduce the risk of frauds and attacks.

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: AISP (Account Information Service Provider – see Figure 3) and PISP¹⁷ (Payment Initiation Services Provider see Figure 4).

¹⁴ Directive 2015/2366

¹⁵ Directive 2007/64/EC

¹⁶ ASPSPs: Account Servicing Payment Service Providers provide and maintain (current, savings and card) accounts, traditionally the core business of a bank.

¹⁷ AISP: Account Information Service Provider - Any (financial) 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 organisation (like a retailer) that can initiate credit transfers on behalf of a client.

3.1.2 PSD2 and GDPR

Although both the GDPR²⁰ and PSD2 share the same objectives – to put customers in control of their own data and to keep that data safe – because they were designed independently of each other, 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 the EDPB's guidance, PSPs must comply with both PSD2 and the GDPR. This means that PSPs could also use the legal basis provided by the GDPR as PSD2 is not a special legislation.²¹

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. 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.²²

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 PSU²³ 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 AISPs and to PISPs) based on the legal provisions on strong customer authentication. From a GDPR point of view, AISPs/PISPs will process the data of the 'silent parties' based on their and the PSUs' legitimate interest.²⁴

²⁰ Regulation (EU) 2016/679

²¹ [The interplay between PSD2 and GDPR](#), CMS Law-Now, April 2020

²² *ibid*

²³ PSU stands for Payment Services User

²⁴ *ibid*

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 PISPs 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 AISPs, but with an additional condition: “in accordance with data protection rules”. It is unclear whether this additional obligation imposed on AISPs 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 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.²⁵

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 respects 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’²⁶ 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*’. It references the steps made since 2014 in terms of the GDPR establishing a framework for digital trust, the Cybersecurity Act²⁷ and the Open Data Directive²⁸: 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 Global²⁹ 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

²⁵ *ibid*

²⁶ 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

²⁷ Regulation (EU) 2019/881

²⁸ Directive (EU) 2019/1024

²⁹ <https://mydata.org>

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.

3.1.4 Summary

All in all, there are unresolved issues³⁰, 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.

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.

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

³⁰ See section 3.3

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 PSD2³¹ which is forcing all 4,000 banks in 27 Member States³² 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 (SCA), the elements that must be employed here, the exemptions, are described over many chapters by PSD2 itself - and several EBA (European Banking

³¹ [Payment Services Directive 2](#): Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EC and Regulation (EU) No 1093/2010 repealing Directive 97/5/EC

³² 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.

Association) RTS³³, Guidelines and FAQs. Also, non-PSD2 regulations, notably GDPR³⁴, 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, financial assets and reputation.

3.3.2 What could go wrong?

It's not difficult to envisage a scenario where a bank simply does not trust a TPP³⁵ 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 on the ThreatMetrix Digital Identity Network in Europe. European digital businesses were hit with 80 million fraud attempts, as they experienced 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 compared with 2017. There is a particular focus on identity testing activities targeting this sector, with fraudsters looking to capitalise upon the low-friction

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

³⁴ [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)

³⁵ 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.

approach taken by many merchants aimed at increasing online revenues and encouraging customer loyalty in a fiercely competitive market.³⁶

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”³⁷. 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 can’t be easily recognised or intercepted by the banks.

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 online³⁸. 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 extension of the problem outlined immediately above.

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

³⁶ 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=

³⁷ <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

³⁸ 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.

PSD2³⁹ 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

Although the lack of a standard and universally applied API in Open Banking is a barrier to greater harmonization in Europe and beyond, it also poses security risks.

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**, 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.⁴⁰
- **Shadow APIs published out of sight of 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.

³⁹ 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

⁴⁰ 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 corporates⁴¹ 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.

⁴¹ 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 months⁴². 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.
- For the **regulator**:
 - Although PSD2 and the various resultant open banking initiatives have received considerable enthusiasm from FinTechs and most banks, the general public does not fully

⁴² 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](#)

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 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 infiltrating an organisation.
 - **Disgruntled or desperate customers**, who are driven to take advantage of access to a bank or finance company for financial gain
 - **Irrational individuals** 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 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.

3.5.1 State of the Art

3.5.1.1 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 and IATA, 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 computing⁴³, are getting closer, and data breaches are exploding⁴⁴.

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. 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 Banking⁴⁵.

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.

⁴³ See 'Disruptive technologies' below

⁴⁴ <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=Accord ing%20to%20researchers%2C%208.4%20billion.saw%20only%204.1%20billion%20exposed>

⁴⁵ <https://blogs.lexisnexis.com/fraud-and-identity-in-focus/uk-lockdown-sees-rise-in-open-banking-cyber-fraud/>

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 services⁴⁶. 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.

3.5.1.2 The Bad News

3.5.1.2.1 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.

3.5.1.2.2 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.

3.5.1.2.3 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 SCA (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).

⁴⁶ <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>

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.

3.5.1.2.4 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 resolve any disputes between stakeholders rapidly and in the customer’s interest, and is developing the system forward as needed. This means that UK has a flourishing Open Banking ecosystem, with ever increasing traction⁴⁷.

Half of 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. The divergence between the UK and the European mainland continent can be expected to be exacerbated after Brexit (see separate paragraph).

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, R2P⁴⁸ 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.

3.5.1.2.5 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 and apps. 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

⁴⁷ <https://thefintechtimes.com/18bn-saving-open-banking/>

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

⁴⁸ Responsibility To Protect: <https://www.un.org/en/genocideprevention/about-responsibility-to-protect.shtml>

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 3.5.8.2.

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 Bluecode⁴⁹) are 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 everyone knows (see also the recent poll at an international European conference), are based on the smartphone, not on cards.

3.5.1.2.6 Flagship projects

At the launch of Open Banking in Europe, while many were still wondering what this might be used for, Deutsche Bank and 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.⁵⁰

After the fanfares, this project—like a few other highly promoted flagships—sadly no longer seems to be 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.

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.

3.5.1.2.7 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

⁴⁹ <https://www.trendingtopics.at/bluecode-ceo-christian-pirkner-in-europa-sind-wir-wirklich-an-allerletzterstelle/>
“Europe is in the last position”

⁵⁰ <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>

Gibraltar⁵¹, clusters of blockchain start-ups in Malta⁵², and many US giants setting up their European headquarters in Luxembourg (PayPal), Lithuania (Revolut) or Ireland (Google). The companies show where the 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. 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 3.5.7).

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.

3.5.1.2.8 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 3.5.8.2 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

⁵¹ <https://www.theolivepress.es/spain-news/2017/01/05/how-gibraltar-became-one-of-the-worlds-biggest-gaming-hubs/>

⁵² <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/>

- 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.

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; cloud computing is more mature although the increasing dependence on US cloud services is a cause for some concern; and many further technological developments are in the making.

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 3.5.8.2 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), IoT⁵³ (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.

3.5.1.2.9 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

⁵³ IoT stands for the Internet of Things.

PKI security⁵⁴. For security applications this means that RSA⁵⁵ 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).

3.5.1.2.10 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 rewarding⁵⁶. 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, Equifax⁵⁷), 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 snapshots⁵⁸ 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.

3.5.1.3 The Good News

3.5.1.3.1 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 tool⁵⁹ 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.

⁵⁴ 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.

⁵⁵ 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.

⁵⁶ <https://www.marketwatch.com/story/identity-theft-is-skyrocketing-and-getting-more-sophisticated-2018-02-27>

⁵⁷ <https://www.bbc.co.uk/news/business-41192163>

⁵⁸ For example, <https://www.securitymagazine.com/articles/91366-the-top-12-data-breaches-of-2019>

⁵⁹ <https://www.eba.europa.eu/single-rule-book-qa>

Examples are a year-long exercise by Visa, where all aspects of secure customer authentication have been defined⁶⁰, including all the many niche use cases. For example, how to:

- make SCA-compliant payments offline (!) at the duty-free cart in an airplane⁶¹;
- 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/car⁶²

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 – 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 shoppers⁶³.

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

3.5.1.3.2 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.

⁶⁰ <https://www.visa.co.uk/partner-with-us/payment-technology/strong-customer-authentication.html>

⁶¹ https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4740

⁶² For example, https://help.twitch.tv/s/article/updating-payment-information-transaction-history?language=en_US

⁶³ 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/>

3.5.1.3.3 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: AML⁶⁴-checks, ATF⁶⁵-checks, FATF⁶⁶-checks, limit-checks will now need to be done in real time and with the same accuracy and better 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.

3.5.1.3.4 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.

⁶⁴ Anti-Money Laundering

⁶⁵ Bureau of Alcohol, Tobacco, Firearms and Explosives (<https://www.atf.gov/qa-category/national-instant-criminal-background-check-system-nics>)

⁶⁶ Financial Action Task Force (<https://www.fatf-gafi.org/>)

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:



Figure 5: Overview of elements of API scheme ⁶⁷

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.

3.5.1.3.5 Data

One of the biggest initiatives of the new Commission is that it has published a whole slew⁶⁸ of documents (A European Strategy for Data⁶⁹, Data Governance in Europe⁷⁰, Retail Payment Strategy⁷¹, Financial Services Strategy⁷², Data Act, etc.) that are pushing the banking industry – and now also other industries – into wider data sharing and hence new security challenges.

⁶⁷ Source: M. Salmony, published since 2014, above diagram updated from <https://informaconnect.com/payments-international/speakers/michael-salmony/>

⁶⁸ <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy>

⁶⁹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066>

⁷⁰ <https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-data-governance-data-governance-act>

⁷¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0592>

⁷² https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en#:~:text=The%20strategy%20sets%20out%20four,including%20enhancing%20the%20digital%20operational

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).

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.

3.5.1.3.6 Blockchain

While the hype around Bitcoin has largely died away, it does continue to play a significant role for speculators (changing from USD 5,000 to USD 20,000 and back again, often in a short time) 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 2017⁷³) 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 equipment⁷⁴, 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 Steria⁷⁵.

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.

3.5.1.3.7 eIdentity

The EU is at last placing more emphasis on eIdentity, recognizing 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 sand⁷⁶.

Since Europe’s flagship identity project eIDAS (electronic IDentification, Authentication and trust Services) is proving to gain limited traction, one can sense a reset in the thinking by the Commission on the best approach towards digital identity. The future is not only in government-issued identity but will be in a federated approach where attributes of people and things are verified.

⁷³ https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

⁷⁴ <https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/#:~:text=On%20Friday%2012%20May%202017,been%20attacked%20before%2012%20May>

⁷⁵ <https://www.finextra.com/newsarticle/37020/sopra-steria-to-take-multi-million-euro-hit-on-ransomware-attack>

⁷⁶ The Age of Consent, The Case for Federated Bank ID, Citi - <https://www.citi.com/tts/insights/articles/article77.html>

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).

3.5.2 Final Goal

Despite being the apparent cornerstone of Open Banking, Open APIs are not Open Banking. Open Banking only comes when all the participants in the ecosystem agree on a **standard** that binds together all definitions and all Open Banking efforts worldwide.

Hence, the dream is of a global Open Banking standard. One API to rule them all. One common way to bind together all the world's banks so that, instead of being confusing, opaque and expensive, banking becomes simple, clear and empowering. Best of all, everyone has access through the use of open standards.

If all the world's banks embraced Open Banking, it would allow them to create intuitive apps that work in the background, anticipating customer needs and offering holistic financial advice. These apps would be driven by algorithms that work best when they have access to the right data and a standard that allowed data to be passed around.

Without the transition to fully-functioning Open Banking worldwide, customers will be limited in the financial decisions they can make and the products and services they can use, rather than being empowered to make choices in relation to their own financial data.

3.5.3 SWOT Analysis

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

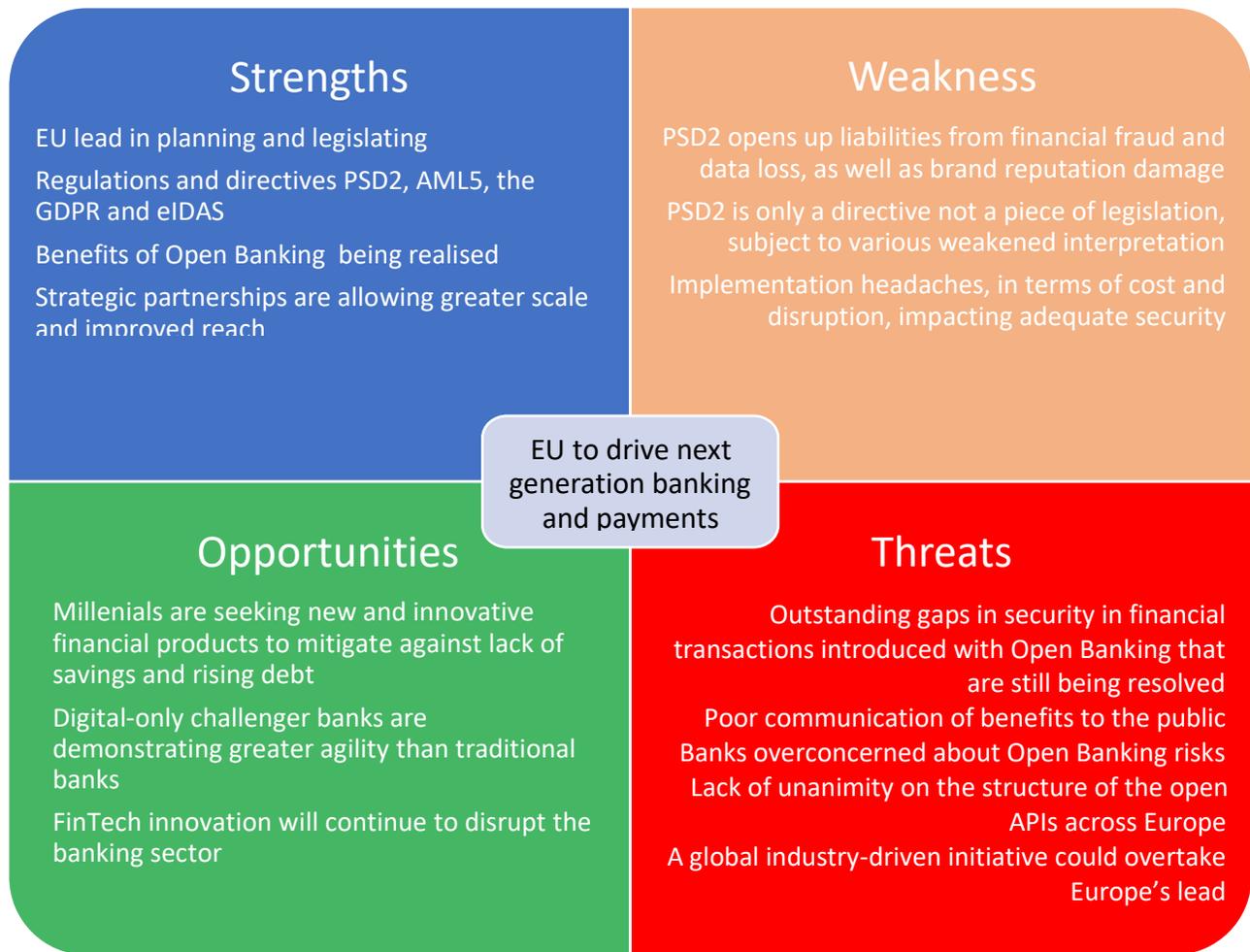


Figure 6: Open Banking SWOT Summary

3.5.3.1 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 accounts⁷⁷

⁷⁷ <https://www.retailbankerinternational.com/news/saga-goldman-sachs-marcus-roll-out-two-savings-products/>

- CYBG and Go Compare partnering for energy switch services in the price comparison world⁷⁸
- consumer brands such as the AA partnering with the personal loan marketplace platform, Monevo⁷⁹
- in the US, the bank Wells Fargo & Company entered into a data exchange agreement with Envestnet | Yodlee, a leading financial data aggregation and analytics platform⁸⁰

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

3.5.3.2 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 is no authority 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, mostly made up of poor quality APIs that have in fact made banking **more** difficult.
- 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 banks⁸¹ have introduced a developer portal or API marketplace that allows any third-party developer to use the APIs a bank has developed

3.5.3.3 Opportunities

One of the stark realities of the 21st 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.

⁷⁸ <https://www.insider.co.uk/news/cybg-industry-first-energy-switching-18211702>

⁷⁹ <https://www.fairinvestment.co.uk/aa-car-loan/>

⁸⁰ <https://www.businesswire.com/news/home/20200924005156/en/Wells-Fargo-and-Envestnet-Yodlee-Sign-Data-Exchange-Agreement>

⁸¹ For example, Nordea: <https://developer.nordeaopenbanking.com/> and <https://www.openbankingtracker.com/provider/nordea>

- As a consequence, millennials 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 banks⁸², 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.

3.5.3.4 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. In a survey carried out in the UK 12 months after open banking was launched⁸³, 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.
- (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 AISP/PISPs to collaborate with them – a clear example would be the adoption of singular APIs.
- (4) 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.
- (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

⁸² It is projected that in the UK high street branches will no longer exist by 2032 - <https://www.asktraders.com/analysis/bank-in-crisis/>

⁸³ 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.

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.

3.5.4 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
Singapore	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.
Hong Kong	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.
China	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.
Japan	Regulatory	Banking Act	2018 – Revised Banking Law (2017 initial release) <ul style="list-style-type: none"> 2018 amendments set requirements for FI/FinTech partnerships to formalise registration rules, standards, and 	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

			development of open API systems by June 2020		
Brazil	Regulatory	Monetary Authority	In four stages between November 2020 – October 2021 ⁸⁴	Brazil is the largest FinTech market in Latin America – fifth in the world - with about 400 companies. Investment in Brazilian FinTech companies totalled about USD52 million in 2015, reaching USD 1.6 billion in 2019	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 concepts in collaboration with TecBan, an established multi-bank and multi-access platform
Australia	Regulatory	Customer Data Right (CDR) legislation	2019 (August) <ul style="list-style-type: none"> • CDR gives customers control of their data and enables them to share it with third-parties (similar to GDPR) • Data Standards Body (DSB) – lays foundation for cross-industry data sharing 	Top four FIs must comply by February 2020. Smaller FIs must comply by February 2021.	No examples available.
New Zealand	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.

3.5.4.1.1.1 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;

⁸⁴ 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 should be implemented by November 2020.
- **Phase II:** Sharing of customers’ registry information and transactional data related to the products and services listed in Phase I, to be implemented by May 2021.
- **Phase III:** Sharing of payment transaction initiation services and forwarding loan proposals, to be implemented by August 2021.
- **Phase IV:** Expansion of the scope of data covered, including foreign exchange operations, investments, insurance, and more. This phase should be implemented by October 2021, making Open Banking fully operational in Brazil.

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.

- 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 (CBDC⁸⁵) in competition with commercial banks⁸⁶.

Many market observers expect CBDC to be inevitable (see Lagarde⁸⁷).

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.

⁸⁵ Central Bank Digital Currency

⁸⁶ 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”

⁸⁷ <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.”

3.5.5 COVID-19 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 surface⁸⁸.

3.5.5.1 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.

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 clients⁸⁹. 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.

⁸⁸ Heightened online spending will cause fraud to increase at an exponential rate, LexisNexis, November 2020

⁸⁹ <https://www.validis.com/wp-content/uploads/2019/08/SantanderCaseStudy2019.pdf>

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 cloud⁹⁰.

3.5.5.2 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.

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

⁹⁰ 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.”

- Evidence of an increase in identity spoofing and first party fraud targeting some e-commerce merchants.⁹¹

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 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.

3.5.6 Green Deal Dimension

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.

⁹¹ 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>

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.⁹²

3.5.7 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) will now need to be revoked and replaced with a national solution. In July 2020, the EBA announced that eIDAS certificates of UK TPPs would be revoked when the Brexit transition period ends on 31 December, 2020. eIDAS certificates are required for TPPs 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 TPPs to use an alternative to eIDAS certificates to access customer account information from account providers, or initiate payments. Companies are expected to ensure that they can continue to provide Open Banking services. The changes will mean:
 - UK-based TPPs will have to obtain a new certificate to be able to continue to provide Open Banking services in the UK, post-Brexit
 - AISPs and PISPs (e.g., banks) will have to make technical changes to their systems to enable TPPs to continue accessing customer account information, by accepting an alternative certificate and informing TPPs as soon as possible which certificate(s) they will accept

In an acknowledgement of the challenges faced by the industry, the FCA is providing 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 will cease. Those who have a Revolut account are already feeling the major consequences of this personally (many emails sent to all customers about how the UK banking licence is being transferred to Lithuania, with IBANs⁹³ 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.

⁹² The European Green Deal, section 2.1.1., Increasing the EU's climate ambition for 2030 and 2050

⁹³ IBN: International Bank Account Number

3.5.8 Sector-specific Dimensions

3.5.8.1 The United States

The United States is where Open Banking really began: American FinTechs have been building applications for decades that allowed financial institutions (FIs) 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. In August 2019, the US Department of the Treasury published a report⁹⁴ 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.⁹⁵

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 Principles⁹⁶ 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

⁹⁴ 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>

⁹⁵ 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."

⁹⁶ https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf

“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 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 regulated⁹⁷, 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 principles⁹⁸. 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.

3.5.8.2 Asia

In Europe the focus is still very much on cards⁹⁹ - 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

⁹⁷ [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.

⁹⁸ [Financial Data Exchange Refines Vision for Consumer-First Financial Data Sharing Practices](#)

⁹⁹ 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

no longer on the physical piece of plastic, but still employs the old rails with 16-digit car 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. 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 users¹⁰⁰. 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

response EPI (European Payment Initiative) which is setting up a pan-European *card* scheme and wallet

¹⁰⁰ See sample statistics under <https://www.chinainternetwatch.com/tag/alipay/#:~:text=Alipay%20is%20China's%20leading%20online,the%20course%20of%20a%20year>.

population – all. That is why it is pervasive and hence also the method of choice for exchanging money (P2P via app¹⁰¹).

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), 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 ¹⁰².

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.” ¹⁰³ Which is rather a different story to introducing a new plastic card in Europe!

3.5.9 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

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)

¹⁰¹ 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.

¹⁰² Although some, even the Chinese government, are becoming increasingly wary of the dominance of these platforms

¹⁰³ Source: <https://www.linkedin.com/pulse/what-super-app-sidu-ponnappa?articleId=6570584548118228993>

JRC Cybersecurity Domain: Security Management and Governance

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

JRC Sectorial Domain: Financial

- Banking services

3.5.10 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

3.5.11 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 regimes¹⁰⁴ and different courts have different interpretations of legislation, primarily, but not exclusively, associated with PSD2.

¹⁰⁴ As PSD2 is a directive, it means that there are 27 national translations of the law

- **Protocols and APIs:** Italy's RI.BA¹⁰⁵ and Bolletino payment schemes use different protocols to those of iDeal¹⁰⁶ 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)** 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** 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.
- ***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 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;

¹⁰⁵ 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 \(RID\)](#)

¹⁰⁶ [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.

- 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

3.5.12 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

3.5.13 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

3.5.14 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

3.6 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.

3.7 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

3.7.1 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).

3.7.2 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.

3.7.3 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 al¹⁰⁷. In addition, it is vital that a common European approach to harmonising standards is taken to a global level, principally with FAPI¹⁰⁸ 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.

3.7.4 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-oriented interfaces and tools, that in so doing provide users with confidence that it is also GDPR compliant.¹⁰⁹

Tools: A number of tools address different aspects of this challenge: Mobile pABC¹¹⁰ (D3.1, Section 5.1), HAMSTERS, PetShop (D3.1, Section 3.6), Guidelines for GDPR compliant user experience (D3.1, Section 3.7)

3.7.5 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.

¹⁰⁷ These include similar initiatives such as those in [Poland](#), [Slovenia](#) and [France](#).

¹⁰⁸ [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.

¹⁰⁹ Although clearly impactful on Open Banking, this solution is not virtual specific.

¹¹⁰ ABC stands for Attribute-Based Credentials

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).

3.7.6 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
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.

3.8 Roadmap

3.8.1 12-month plan

The challenges identified at 3.5.9 and 3.7.1 and considered important for the first 12 months of the project have still yet to be resolved. Hence, over the next 12 months, focus needs to be applied to 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 being built.

From this, it is to be expected that a number of gaps in security and privacy will become apparent, leading to a number of methods and approaches to ensure closure.

3.8.2 2-year (or until the end of the project) plan

By the end of 2022, we should have been able to investigate:

- The impact of the discontinuation of relationships in an established trust chain across the various scenarios envisaged in the 12-month plan
- 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 jurisdictions based on the challenges outlined in 3.5.11 and 3.7.3

3.8.3 Beyond the end of the project

There are some further potential security areas to address that perhaps will only be addressed after the end of the project:

- **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

¹¹¹ [Electronic identification and trust services](#): Regulation (EU) No 910/2014 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

- **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 checkouts.

3.9 Summary

This section focusses on security considerations associated with Open Banking. 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 3.5.3) 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 ICT¹¹²” 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 information technology (IT), makes the protection of each of its elements extremely difficult, even almost impossible.

¹¹² ICT stands for Information and Communication Technologies

As the saying goes, “Security 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 operational technology (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 ISO¹¹³ 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.

¹¹³ ISO stands for International Organization for Standardization

- *Supporting services*: Storage and archival of information, Product and vendor certification.

As for the **assets** that comprise the supply chain ecosystem, this 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, RFID¹¹⁴ labels...), *IT Networks and components* (facilities networks, supply chain collaboration networks, network components), *OT¹¹⁵ 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:

¹¹⁴ RFID stands for Radio-Frequency IDentification

¹¹⁵ OT stands for Operational Technologies

- 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 to 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 twin** is 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”¹¹⁶.
- In 2018, Ericsson suffered from an unintentional supply chain attack: An expired certificate on Ericsson devices/software – “[...] because of a faulty software [...]”¹¹⁷ – caused network outage

¹¹⁶ <https://csr.asus.com/english/article.aspx?id=1741>

¹¹⁷ <https://www.ericsson.com/en/press-releases/2018/12/update-on-software-issue-impacting-certain-customers>

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.

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 NIST¹¹⁸ [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.

¹¹⁸ NIST stands for National Institute of Standards and Technology

- *Damage to or of 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 be 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 people¹¹⁹, weapons, and illegal substances^{120 121}, theft¹²², and various digital threats such as digital skimming¹²³ and theft of personal information¹²⁴. *Terrorists* have also tried to abuse the supply chain to perform acts of terror¹²⁵. All *intelligence services* have also participated in the manipulation of the products and services of both

¹¹⁹<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>

¹²⁰<https://www.bbc.com/news/world-europe-25640485>

¹²¹<https://www.bbc.com/news/world-europe-24539417>

¹²²https://onlinelibrary.wiley.com/doi/pdf/10.1111/dec.12336?casa_token=ifPZDxYdAwQAAAAA:jU0gYtsIT0fFOIOT3V5ozqHZQrrQW328jTZsVuK16QCQhBuSPFAeasxZtfSkqVQQ1enFvcBHASnXFXE

¹²³<https://blog.trendmicro.com/trendlabs-security-intelligence/new-magecart-attack-delivered-through-compromised-advertising-supply-chain/>

¹²⁴<https://research.checkpoint.com/2019/operation-sheep-pilfer-analytics-sdk-in-action/>

¹²⁵<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>

hardware¹²⁶ and software¹²⁷ 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 / mismanagement¹²⁸.

As a result of our analyses, we have observed that most of the 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.

4.5 Research Challenges

4.5.1 State of the Art

The first version of the CyberSec4Europe “Research and Development Roadmap” [Markatos 2020] (i) provided an overview of the elements that are at stake within the supply chain context, (ii) described the potential attackers who target them, and (iii) outlined the most important challenges related to the security of supply chains—including the detection and management of supply chain security risks, the security hardening of supply chain infrastructures, the security and privacy of supply chain information assets and goods, and the management of the certification of supply partners. As with other verticals in this version of the “Research and Development Roadmap”, this subsection provides the results of research into the state of the art of supply chain security with respect to these research challenges.

4.5.1.1 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 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 2020, 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]). Other standards, such as ISO 31000:2018 [ISO31000 2018] and the various NIST Special Publications, such as NIST SP 800-161 [NIST 2020b], provide the foundation to manage risks in supply chain ecosystems. These standards consider not

¹²⁶<https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies>

¹²⁷ <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>

¹²⁸<https://www.theguardian.com/uk/2013/feb/15/horsemeat-scandal-the-essential-guide#101>

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 2020B] and private companies like Accenture¹²⁹, 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 unchecked¹³⁰. 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 of 2020, 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.

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 [NFW 2017]. 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 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. Also, in [PS 2008], the authors provide a tool that builds attack graphs using data obtained from maritime supply chain infrastructures—more specifically, information from network and information service assets that belong to different supply chain actors. This information is, in turn, processed with vulnerability databases to create an attack tree that will be analysed using recommender systems. However, the compilation of assets still requires manual intervention, and the prediction and forecasting methods need more improvements.

¹²⁹ <https://www.accenture.com/acnmedia/pdf-107/accenture-security-cyber.pdf>

¹³⁰ <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

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 [PS 2008]. 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.

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 [ZB 2012], the authors make use of a game-theoretic approach to model the interactions between cybersecurity policies and the physical interactions of the infrastructure, so as to discover the optimal equilibrium of cyber defence policy and robust control design. 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. Also, 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. 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.

4.5.1.2 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 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, the few research advances made in this line present an immature state [GSC+ 2017] [CRF+ 2018]. Most of the proposed approaches to prevention, detection and response focus primarily on offering reactive methods rather than proactive solutions, without going further and looking at how to avoid adverse situations in time, or how to eradicate or mitigate possible (collateral) effects. 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).

Many of the technologies that are being adopted to improve the quality of the service 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 centralise the main security actions in a cloud server (e.g. authentication [PSvS 2019] [LSC 2015], access control [PSvS 2019] [LSH+ 2011]) or distribute them throughout the entire system (e.g. distributed detection [HAP+ 2016]).

Clearly, working with powerful technologies such as cloud computing requires further research, not only at the perimeter level but also at the computing and storage level—mainly because cloud platforms are vulnerable to compliance violations and cybersecurity issues [HCG+ 2020]. At perimeter level, Software Defined Networks could be a suitable mechanism to reduce an organisation's attack surface [O'Raw 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.

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*. 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 [HCG+ 2020] 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]). In this process, it is recommended to protect the data life-cycle [HAP+ 2016] and intensify security audits to minimise the risks and detect misuse or abuse of the techniques, especially when these are able to get access to private Supply Chain data. Bad use of these data warehouses can significantly impact on the privacy of an organisation or may alter the integrity of the data.

Blockchain is another relevant technology that can be adapted to the Supply Chain sector for multiple proposals, and particularly for prevention and detection. 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 IIoT¹³¹/CPS/IoT, to create an interoperable and secure industrial environment. For this interoperability level, the work [GPV 2019] proposes to apply Deep Learning Smart Contracts for authentication of devices with support for Deep Autoencoder for anomaly analysis. This enables the development of highly accurate classification or correlation models, which are very useful for anomaly detection during the IIoT communications. This interconnection capacity can even foster the need to create federated environments that support the sharing of threat and vulnerability repositories [CSP+ 2020].

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

¹³¹ IIoT stands for the Internet of Industrial Things

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 [HCG+ 2020]. 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].

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 Chain partners to increase their level of resilience [KKV 2013] [ASA 2018] [YI 2019], 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. Unfortunately, this kind of intelligence, and particularly Cyber Threat Intelligence (CTI) in Supply Chain, is in its early stages of maturity [Yeboah-Ofori 2019], in which it is still necessary to create secure common access platforms to share events, threats, security risks and incidents.

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]. In addition, its 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].

4.5.1.3 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)¹³². These benefits and various regulatory requirements in sectors such as food networks [CSH+ 2014], pharmaceuticals¹³³, and clothing¹³⁴ have provided a boost to research and development in this 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 semantics¹³⁵. 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].

One approach to overcome this hurdle is to make use of *common technological solutions* to facilitate the implementation and deployment of data sharing processes. 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 standards¹³⁶ 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 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.

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 also it is possible to provide private information repositories where only a subset of the members are authorised to access the data. Additionally, deterministic smart contracts can be used to define the business logic of

¹³² https://www.bsr.org/reports/BSR_UNGC_Guide_to_Traceability.pdf

¹³³ <https://www.who.int/medicines/regulation/traceability/7OCT19draft-WHO-policy-brief-on-Traceability-of-Health-Products.pdf>

¹³⁴ https://www.unece.org/fileadmin/DAM/trade/SustainableTextile/2020_April_Webex/Draft_Mapping_of_Regulations_Policies_and_Guidelines_for_TT_22.04.20.pdf

¹³⁵ <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=15354>

¹³⁶ <https://www.gs1.org/standards/>

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 environmental benefits [GKH+ 2020]. At present, there are already 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]. 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 EPCIS¹³⁷) and with IoT infrastructures [QTB 2019].

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)* [Mühle 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 2020, 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) and [BVH+ 2019] (decentralised peer-to-peer trust marketplace that connects SSI owners with regulatory compliant service providers).

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]. Moreover, as Blockchain is still a largely unexplored technology, its own security challenges are beginning to be identified, including attacks against the blockchain structure, peer-to-peer system and applications [SSN+ 2020], plus attacks against the authentication infrastructure in permissioned systems [DSL 2018]. 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.

All the previous paragraphs have focused on sharing information related mostly to physical assets. However, we also have to consider that digital assets are part of supply chains and, as such, they also need to be tracked and managed. This is especially important given the use of open-source components in software infrastructures: among modern applications today, 90% of the average codebase is composed of open-source

¹³⁷ <http://info.rfid.auburn.edu/chip-proof-of-concept-results>

components, yet 11% of such components are either obsolete or contain vulnerabilities [Sonatype 2020]. Moreover, the number of attacks actively targeting open-source software projects increased by 450% from July 2019 to May 2020 [Sonatype 2020]. These growing threats have 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. Still, the notion of an SBOM attached to every component is still in its infancy, as it is still necessary to define several aspects of this concept—including what contents a SBOM should have, what tools are needed to automatically exchange this information, and others [Martin 2020]. Moreover, there are additional issues to be solved, such as the granularity of an SBOM: many vulnerabilities are associated with specific libraries/modules that might be hidden within several layers of components, yet a fully defined SBOM might include thousands of components, whose vulnerabilities might not even be exploitable because of the design of the application¹³⁸. There are other solutions that can be applied to this context, such as the continuous validation of components and interconnections through vulnerability analyses, and the specification of open architecture software ecosystems where a set of components are tested and validated as a whole [SA 2018].

4.5.1.4 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. 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 [WHO+ 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 standards¹³⁹, 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 2019¹⁴⁰, 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

¹³⁸ <https://cybersecurity.att.com/blogs/security-essentials/software-bill-of-materials-sbom-does-it-work-for-devsecops>

¹³⁹ <https://www.isa.org/standards-and-publications/isa-standards/>

¹⁴⁰ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0477&from=EN>

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”)¹⁴¹. As of 2020, the work on all these areas (development of EU certification schemes, certification composition) is still ongoing.

However, we have to consider that compliance with security certifications might not guarantee security assurance [DW 2014]. 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 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].

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 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]. 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 processes¹⁴². 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 bodies¹⁴³ 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.

¹⁴¹ <https://ecs-org.eu/documents/uploads/product-composition-document-november-2020.pdf>

¹⁴² <https://cloudsecurityalliance.org/artifacts/star-continuous-technical-guidance/>

¹⁴³ <https://www.intertek.com/cyber-assured/>

Precisely 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 technologies, such as the automatic extraction of Manufacturer Usage Descriptors (MUD) through automated IoT security testing methodologies [MRP 2019], 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].

4.5.2 Final Goal

Although it is impossible to achieve perfect cybersecurity against supply chain threats, given the dynamic nature of this ecosystem, the final goal of the research into supply chain security is to create an environment where operations are performed in a secure and private way, where vulnerabilities are minimised, and where attacks are promptly discovered and managed. By improving supply chain risk management (SCRM) processes and by implementing continuous certification, all supply chain actors will be able to participate in a trusted ecosystem where potential risks are identified and can be carefully monitored. Clearly, the cybersecurity tools that will check for the presence of potential risks will not work in isolation, but must interact with each other to prevent, detect, and react against threats. Within this collaborative environment, all actors will make use of various tools that facilitate the secure and private exchange of information with each other. Such tools will not only provide support to existing supply chain processes in a more secure and private way, but also enable novel services such as event management and real-time transparency about the origin and processing of physical and digital assets.

4.5.3 SWOT Analysis



Figure 7: Supply Chain SWOT Summary

In our globalised economy, supply chains are built internationally. 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.

The need to set up supply chain securely is demonstrated by the fact that numerous attacks have taken place in the past, as mentioned in the state-of-the-art section. In particular, a recent MIT report¹⁴⁴ mentions that "supply chain attacks rose by 150% between 2016 and 2017". Also, a 2019 report points out that risk-based approaches have proved to be suitable for addressing cybersecurity threats to supply chains¹⁴⁵. Beyond that

¹⁴⁴ <https://mitsloan.mit.edu/sites/default/files/2020-02/Supply%20Chain%20-%20ROUNDUP-DESIGN-5.pdf>

¹⁴⁵ https://www-file.huawei.com/-/media/corp/facts/pdf/2019/huawei-white-paper_tony-scott_final.pdf?la=en

the author 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.

A summary of the supply chain SWOT analysis is presented in Figure 7. Detailed SWOT analysis results are presented below.

4.5.3.1 Strengths

- The EU’s **financial and economic power** make the Union a major player (with regard to both producers and consumers of goods) in the world: 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 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 billion¹⁴⁶ to ensure Europe’s competitiveness. Concerning supply chain security, the EU and its partner countries has become aware of security challenges through supply chain attacks¹⁴⁷ in the past and has created and funded projects to react and be prepared in this regard e.g. Customs Detection Technology Project Group (CDTPG), SecureSCM¹⁴⁸, Cybersec4Europe¹⁴⁹, etc. In total, the EU has produced over 2000 project deliverables and publications in the supply chain domain.
- The economy of the EU has **leadership 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], healthcare¹⁵⁰ and Industry 4.0 [ENISA 2019A], and for secure ICT procurement of electronic communications [ENISA 2014].
- Many EU organisations and companies are part of the Open Trusted Technology Forum¹⁵¹ (OTTF), whose aim is to increase product integrity and supply chain security by developing **open standards and certification programs**.

4.5.3.2 Weaknesses

¹⁴⁶ <https://ec.europa.eu/programmes/horizon2020/what-horizon-2020>

¹⁴⁷ <https://ec.europa.eu/digital-single-market/en/news/overview-supply-chain-security>

¹⁴⁸ <https://cordis.europa.eu/project/id/213531>

¹⁴⁹ <https://cybersec4europe.eu/ensuring-the-security-and-integrity-of-supply-chains/>

¹⁵⁰ https://www.enisa.europa.eu/events/5th-ehealth-security-conference/presentations/Procurement_Guidelines_for_Cybersecurity_in_Hospitals.pdf

¹⁵¹ <https://www.opengroup.org/forum/trusted-technology-forum>

- 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 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.

4.5.3.3 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) 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 report¹⁵² 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 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).

¹⁵² https://www-file.huawei.com/-/media/corp/facts/pdf/2019/huawei-white-paper_tony-scott_final.pdf?la=en

- As trust in product quality is a key reason for customers to buy, **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.
 - When intra-EU integration via a common supply chain management standard/"Euro-blockchain" increases, this allows greater variability and access to suppliers and customers across the EU.
 - There are strong competitive advantage for EU companies in certain sectors as global suppliers become more integrated

4.5.3.4 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**.

4.5.4 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 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.

4.5.5 COVID-19 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 of the supply and demand. Demand for things like personal protective equipment and toilet paper has risen sharply, while the demand for cars and office toilet paper has fallen dramatically. At the same time, the supply was affected either 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 effects caused by the COVID-19 pandemic on the supply chains is also shown by the McKinsey survey of global Supply Chain leaders (performed in May 2020)¹⁵³, 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

¹⁵³<https://www.mckinsey.com/business-functions/operations/our-insights/resetting-supply-chains-for-the-next-normal>

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 manufacturing¹⁵⁴. 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 company Nike¹⁵⁵ 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 the disease between communities. It is therefore essential to track their movement and possible signs of sickness while maintaining their privacy.

The COVID-19 crisis has also directly impacted the security of supply chains¹⁵⁶. 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 being able 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.

But 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

¹⁵⁴<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>

¹⁵⁵<https://www.mckinsey.com/business-functions/operations/our-insights/covid-19-and-supply-chain-recovery-planning-for-the-future>

¹⁵⁶<https://www.sme.org/technologies/articles/2020/august/ul-says-covid-19-increases-cybersecurity-problems/>

and shipping cargo around the world. Two recent examples are the attacks on the shipping company CMA CGM¹⁵⁷ and the International Maritime Organization¹⁵⁸. 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 impersonating, among others, FedEx, DHL and UPS have been detected¹⁵⁹.

4.5.6 Green Dimension

With the European Green Deal¹⁶⁰, 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 report¹⁶¹ 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 on their greenhouse gas emissions more, 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 Chain¹⁶² 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 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.

¹⁵⁷ <https://www.supplychaindive.com/news/cma-cgm-ocean-shipping-malware-cyber-attack-information-technology/585978/>

¹⁵⁸ <https://gcaptain.com/international-maritime-organization-hit-by-cyber-attack/>

¹⁵⁹ <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>

¹⁶⁰ <https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal>

¹⁶¹ [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)

¹⁶² <https://op.europa.eu/en/publication-detail/-/publication/8ba0a8fd-4c83-11ea-b8b7-01aa75ed71a1>

greenhouse gas emissions) that are necessary to show a company's due diligence. Traceability of goods also helps to improve the trustworthiness of companies and customers' trust in the products and services provided. Cybersec4Europe does this by introducing 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. As another example, it can also be used to measure the carbon footprint of products by accumulating the carbon footprint of suppliers' goods, the routes of transportation used and the energy consumed for producing products.

The supply chain vertical is closely related to other verticals, given 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).

4.5.7 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).

4.5.8 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.

4.5.9 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.

4.5.10 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.

4.5.11 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.

4.6 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.

4.7 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.

4.7.1 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 CORAS¹⁶³.

4.7.2 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 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.

¹⁶³ <http://coras.sourceforge.net/>

4.7.3 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 PLEAK¹⁶⁴, can help in selecting specific privacy parameters and policies.

4.7.4 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 methodologies such as CORAS (D3.1, Section 5.2)	Adaptation of recognized SCRM methodologies, lightweight and automated mechanisms for supply chain scenarios

¹⁶⁴ <https://pleak.io/home>

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

4.8 Roadmap

4.8.1 12-month plan

For the next 12 months, we need to focus on the following aspects of supply chain security:

- At present, there are already various tools and mechanisms that can provide penetration testing and software analysis services for supply chain ecosystems. For the **protection of IT/OT infrastructures and networks** and the **compliance with regulations**, it is necessary to *apply such tools to test not only the supply chain infrastructure but also the supply chain goods—both software and hardware (firmware)*. More specifically, the existence of novel certifications and guidelines in this regard will push the integration of such mechanisms into existing supply chain processes over the next year.
- Blockchain is already being used to exchange information related to supply chain events. Thus, the plan for **blockchain-based solutions** in the next 12 months is focused on the *integration of distributed workflow operations management* in supply chains through smart contracts, as there are already blockchain solutions that provide support for the exchange of basic information through blockchains. Therefore, it is now possible to explore the usage of tokens for representing information about a workflow, such as starting business processes only when all necessary tokens are available. The integration of such processes can also facilitate the applicability of accountability processes in case of conflict.

4.8.2 2-year (or until the end of the project) plan

For the next 2 years, we need to focus on the following aspects of supply chain security:

- Regarding the ***protection of IT/OT infrastructure of supply chains***, there are various aspects that can be made available and/or improved in two years' time. For example, there are already various *defence mechanisms* that are based on technologies such as Cloud, physical unclonable functions (PUF), and blockchain, and it is expected that they will be further refined. As for the ***trusted exchange of information***, it is necessary to advance more in the area of *sharing information about software assets*, which will provide a foundation for the security of the software supply chain.
- There is also ongoing work and research on applications that ***facilitate the automation of certain aspects of supply chain risk management programs***. These include, among others, the *specification and analysis of cyber kill chains* that will highlight the weakest points in the supply chain ecosystem, and the definition of *continuous vulnerability analysis processes* that monitor the compliance of certain supply chain processes. It is to be expected that these aspects will be refined in two years' time.
- As for the 2-year plan and the integration of ***blockchain-based solutions***, there are various avenues that can be explored in this period of time. One such avenue is the *integration 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*.

4.8.3 Beyond the end of the project plan

Regarding blockchain-based solutions, ***future solutions could take full advantage of the properties of the blockchain*** to fulfil its goal as a mechanism that can be used to protect the security and privacy of all assets and goods. 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*.

Another avenue of research is related to the supply chain risk management and compliance with regulations, where ***the integration of automatic mechanisms that can continuously analyse and pinpoint potential and/or existing security and privacy issues in all assets*** can be used for several purposes, including: i) the *integration of continuous certification processes* that can attest 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.

Another aspect to take into consideration is ***the availability of autonomous self-healing processes***, which will facilitate the automatic recovery and reconfiguration of states, processes or parameters in IT-OT networks - an essential aspect to guarantee at all times business continuity in (hyper-)connected supply chain networks. One technology that can facilitate this 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: *how to manage the “trust” in the two-way interface*

between the real and physical world, and how to integrate digital twins as part of the IT-OT infrastructure (including technologies such as cloud and IoT) in a secure way.

Finally, the advent of **Artificial Intelligence and Big Data applied to security and privacy of IT-OT infrastructures**, plus other tools such as **threat intelligence sharing**, can provide multiple benefits to supply chain infrastructures, including: i) *optimizing and improving the decision-making processes and response for cyber intelligence*, so as to achieve a better awareness of the situation, and achieve a better governance of the system; and ii) *automatically harden supply chain IT-OT infrastructures* due to the better knowledge of the infrastructure and its risks.

4.9 Summary

This section focused on the security of the supply chain. As explained in section 4.4, the supply chain sector is under attack by criminal organizations, intelligent services, insiders, and even terrorists. These actors can deliver a major blow which, as explained in section 4.3.3, can result in harm to operations, harm to assets, harm to individuals, and potentially even harm to entire nations!

A brief SWOT Analysis in section 4.5.3 showed that EUROPE 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.

Being one of the most necessary sectors, supply chain has been hit hard by the recent pandemic (see section 4.5.5) which not only hindered transportation of people and goods, but also made significant changes to the balance of supply and demand, as demand for health- and hygiene-related goods and services soared beyond any recent predictions. Given the current dramatic situation of the sector, an even modest cyberattack could clearly be a final blow for many places and services.

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 section 4.5.4): 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.

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 (as can be seen in section 4.5):

- 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

Addressing them with a special focus on the infrastructure of the supply chain, the automation of supply chain risk management, and the inclusion of blockchain-based solutions, should be given high priority over the next few years.

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 gives the users the attestations necessary to proof 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.

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 [Declerq 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 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 the 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 eIDs¹⁶⁵) that would provide sufficient trust.

Regulation (EU) 2016/679 of the European Parliament and of the Council, more commonly known as General Data Protection Regulation (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 [Hobson, 2020] half of the companies agree that GDPR compliance is not possible without it. Naturally, the used IdM systems themselves still have to follow the GDPR requirements for compliance to be possible.

Regulation (EU) No 910/2014 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, more commonly known as eIDAS, is a fairly recent regulation on electronic identification and trust services in the European Single Market. The trust services mentioned include electronic signatures, electronic seals, time stamps, electronic

¹⁶⁵ Electronic IDentities

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 that offer an online public service, for which access is granted based on an electronic identification scheme, will also recognize 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 ENISA¹⁶⁶.

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.

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

¹⁶⁶ENISA: "Mobile Identity Management", 2010. Available at <https://www.enisa.europa.eu/publications/Mobile%20IDM>

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.

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 Research Challenges

5.5.1 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 D5.2 [Sforzi 2020].

5.5.1.1 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.

5.5.1.2 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 PRIME¹⁶⁷, FP7 PrimeLife¹⁶⁸, FP7 ABC4Trust¹⁶⁹, H2020 CREDENTIAL¹⁷⁰, H2020 OLYMPUS¹⁷¹, or H2020 ARIES¹⁷², 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.

In the last year, some new works in the field of privacy Attribute-Based Credentials (p-ABC) have been published. [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.

5.5.1.3 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 [Chaum82] (combined with zero-knowledge proofs of knowledge to ensure veracity) or oblivious pseudorandom functions [FM+05] 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) [Agrawal+18] to obtain threshold

¹⁶⁷ <https://cordis.europa.eu/project/rcn/71383/factsheet/en>

¹⁶⁸ <https://cordis.europa.eu/project/rcn/85453/en>

¹⁶⁹ <https://abc4trust.eu/>

¹⁷⁰ <https://credential.eu/>

¹⁷¹ <https://olympus-project.eu/>

¹⁷² <https://www.aries-project.eu/>

oblivious password based SSO. The work by Baum et al. [Baum+20] 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 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 dp-ABCs as one of the complementary solutions for token generation.

5.5.1.4 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 the cryptocurrencies. Proposed works included in [BLZ+ 2020] and [BBC 2019], applies 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.

5.5.1.5 Password-less authentication

Nowadays an average person has 70-80 passwords according to a research conducted by NordPass, which offers password manager solutions [HSMC20]. 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)

Alliance¹⁷³ are constantly gaining popularity. Recently the FIDO standard has been adopted by many big 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 FIDO2¹⁷⁴ 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 protocol¹⁷⁵ and the Client-to-Authenticator-Protocol (CTAP2)¹⁷⁶ 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 [ZG 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 [AWAC 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.

5.5.1.6 GDPR and eIDAS impact interoperability

¹⁷³ <https://fidoalliance.org/>

¹⁷⁴ <https://fidoalliance.org/fido2/>

¹⁷⁵ <https://fidoalliance.org/fido2/fido2-web-authentication-webauthn/>

¹⁷⁶ <https://fidoalliance.org/specifications/download/>

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. Here is a quick rundown of the more prominent such solutions.

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)¹⁷⁷. 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 recommendations¹⁷⁸.

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 tool¹⁷⁹), and the French Commission Nationale de l'Informatique et des Libertés (CNIL) [CNIL]. Other tools have also been developed and shared freely^{180,181}. There have also been good examples of directions for the assessment of specific data processes, which can be adopted for other use cases. Examples are the Privacy by Design and Data Protection Impact Assessment (DPIA) Toolkit by Edinburgh Business School [EBS], and Code of Conduct and DPIA template by Family Links Network [FLN]. There have also been a few projects funded^{182,183}, 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].

5.5.1.7 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

¹⁷⁷ https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

¹⁷⁸ https://edpb.europa.eu/about-edpb/board/members_en

¹⁷⁹ <https://www.enisa.europa.eu/risk-level-tool/>

¹⁸⁰ <https://github.com/simonarnell/GDPRDPIAT>

¹⁸¹ <https://github.com/CSR-AIT/dpia-tool>

¹⁸² <https://localdigital.gov.uk/funded-project/digital-data-protection-impact-assessment-dpia-tool/>

¹⁸³ <https://www.dsfa.eu/index.php/en/home-en/>

[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 5.5.1.2 and 0. 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. [BEF19], 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.

5.5.2 Final Goal

The final goal of the research into Privacy-Preserving Identity Management (ppIdM) is to provide a set of advanced mechanisms that can be integrated in various scenarios, in order to provide additional protection and privacy features to end-users, organizations and infrastructures. Thanks to the provided tool, European systems would be able to perform authentication and authorization processes with strong trust, while enforcing user privacy.

5.5.3 SWOT Analysis



Figure 8: 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 8, while a more detailed explanation of the results comes in the following.

5.5.3.1 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 ABC4Trust¹⁸⁴, H2020 ARIES¹⁸⁵, H2020 OLYMPUS¹⁸⁶) 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**.

5.5.3.2 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**

¹⁸⁴ <https://www.abc4trust.eu/>

¹⁸⁵ <https://www.aries-project.eu/>

¹⁸⁶ <https://olympus-project.eu/>

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;** given that security and privacy are non-tangible, and (hardware) requirements are higher for privacy-preserving solutions, providers may be reluctant to invest the necessary costs.

5.5.3.3 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.**

5.5.3.4 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 are a loose set of rules that **are 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.

5.5.4 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.

5.5.5 COVID-19 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 adopted on 17 April (https://www.europarl.europa.eu/doceo/document/TA-9-2020-0054_EN.pdf) 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 ppIdM technologies envisioned in this project can help against these issues, allowing users to enjoy those digital services without great concern about their privacy.

5.5.6 Green Dimension

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.

5.5.7 Sector-specific Dimensions

Although there are scenarios where privacy protection using technical approaches is more relevant (e.g. ones where there are multiple untrusted services), ppIdM tools are relevant in any scenario where users' digital identity is involved. Specially, in this project there will be a strong collaboration between the ppIdM and Smart Cities verticals, where the results of the ppIdM research will be used as components for the Smart City pilot.

5.5.8 Challenge 1: System-based credential hardening

The identity of a user is bound esoterically 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

5.5.9 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.
- *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

5.5.10 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)

5.5.11 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

- ***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.

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)

5.5.12 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

5.5.13 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 2728 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.

5.5.14 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 amount 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

5.6 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).

5.7 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.

5.7.1 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.

5.7.2 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 challenge is not to develop an identity management system, but to adopt and integrate the existing one.

5.7.3 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.

5.7.4 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. To this end, it is envisaged to use the outcomes from the DIF as a baseline.

5.7.5 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)¹⁸⁷ and the FIDO 2¹⁸⁸ 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.

5.7.6 GDPR guidelines and eIDAS interoperability

These assets asset will investigate the two prominent European regulations regarding privacy and identity management. The first will produce a comprehensive guideline on applying GDRP 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.

5.7.7 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.

¹⁸⁷ <https://fidoalliance.org/specs/fido-uaf-v1.2-rd-20171128/fido-security-ref-v1.2-rd-20171128.html>

¹⁸⁸ <https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.html>

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 cracking hard
Challenge 2	Unlinkability and minimal disclosure	Mobile pABC, eABCs, ArchiStar (D3.1, Section 5.1)	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 Solutions for the IoT	eABCs	

5.8 Roadmap

5.8.1 12-month plan

For the next 12 months, we need to focus on the following aspects of Privacy-Preserving Identity Management:

- **Unlinkability and minimal disclosure.** Improve the p-ABC system that has been proposed to fulfil the unlinkability and minimal disclosure requirements (included in the distributed oblivious identity management system) with range proofs (allowing complex numerical predicates), and other general improvements that increase the maturity of the implementation.
- **Distributed oblivious identity management.** Continue consolidating the distributed oblivious identity management system based on the needs detected in current implementation efforts. For instance, we plan to improve the interoperability of the solution by integrating the p-ABCs with the W3C emerging standards (Verifiable Credentials and Presentations).

- **Privacy preservation in blockchain.** Start the integration of the privacy preserving technologies (specifically, the system devised for distributed oblivious identity management) with blockchain to the point of acquiring a mature implementation that allows demonstration of the main functionality through proof of concept deployments.
- **Password-less authentication.** For the deployment of the password-less authentication solution we are planning to *implement a biometric authentication method that relies on the FIDO protocols and is device-centric*. The previous year, the authentication system's requirements were thoroughly studied, and the system's architecture was designed. Later, a comparison was performed between the different FIDO versions to find the most appropriate based on the current requirements. We concluded that two FIDO versions will be implemented: FIDO UAF and FIDO 2, to expand the system's capabilities to support web authentication. The plan for 2021 is to finish the development of the password-less authentication system, namely the development of the client and server applications that will constitute the authentication system.

5.8.2 2-year (or until the end of the project) plan

For the next 2 years, we need to focus on the following aspects of Privacy-Preserving Identity Management:

- **Distributed oblivious identity management.** The final goal for the 2 plan year is the *deployment of a distributed oblivious identity management system that fulfils the security and privacy requirements*. In this plan, several activities are contemplated. We will continue with tasks involving the design of the system architecture, development of cryptographic components and framework integration. The development of these tasks will be iterative, pilots for the use cases will be deployed and used to evaluate user experience and compliance with legal requirements.
- **Unlinkability and minimum disclosure.** As a short- to medium-term research initiative, the analysis of several additional functionalities for anonymous credential systems is envisioned. For instance, we plan to *design issuer-hiding ABC system*, which only prove that one possesses a credential from one of a set of issuers. Such systems would allow one to prove, e.g., that one possesses a university degree without revealing the issuing institution, thereby directly overcoming challenges of the respective demonstrator case. Another envisioned extension is the *combination of ABC systems with state-of-the-art access control mechanisms*. This would reduce the number of necessary authentication steps of the end user, as she could reveal all information a certain institution (e.g., hospital) might require, while still having formal guarantees that each employee would only be able to access the required amount of information (e.g., doctors would be able to access other parts of the same presentation token than the hospital administration or the patient's insurance company). Reference implementations to demonstrate the efficiency and scalability of these extensions are foreseen.
- **Privacy preservation in blockchain.** For the remaining two years of the project, the plan can be divided in two phases. The first comprises the next 12 months and it is detailed in the previous section. For the last 12 months, we should part from a *mature implementation* with demonstrable core functionalities. Finally, during the third year, the *full integration* should be completed *to accommodate a set of well-defined use cases*, permitting testing and measurement processes that will check and verify the performance and usability of the proposed solution.

- **Password-less authentication.** By the end of 2022 we are planning to perform a pilot usage of the system to improve the user experience process, since usability is regarded as one of the most important attributes of an authentication system. In parallel with the pilot usage, we will focus more on the system's privacy. Particularly, we will integrate an ABC solution to our password-less authentication system to offer privacy-preserving capabilities. From 2023 and beyond, we intend to update the system's features in order to improve its usability by implementing more authenticators (e.g., voice recognition) and meet the needs that will have been arisen at that period.
- **System-based credential hardening.** To address system-based credential hardening, we plan to *incorporate cryptographic services for hardening text-based passwords in the prototype of the distributed oblivious identity management system*. Additionally, we plan to carry out research for *incorporating credential hardening for non-textual credentials*.
- **GDPR guidelines and eIDAS interoperability.** Iterative 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.

5.8.3 Beyond the end of the project plan

The following research challenges will be worked on by CyberSec4Europe partners only after the project duration:

- **GDPR guidelines and eIDAS interoperability.** We have mentioned, the GDPR is a very loose set of rules, often dependent on how the European Court of Justice, the supervisory authorities and often big players in the industry interpret the regulation. All of this is also subject to change over time. This could make the guidelines provided in the project become obsolete. Issues and other findings with the eIDAS interoperability will also change through time. That is why continuous support, even beyond the scope of the project, is necessary.
- **Identity Management Solutions for the IoT.** While the related research activities within CyberSec4Europe have finished after the feasibility result in [HK 2019] by designing a cloud-based privacy-preserving authentication mechanism, mid-term plans include the design of lightweight protocols built (mainly or exclusively) from symmetric primitives, an approach that has been followed, e.g., for group signatures by Boneh et al [BEF19].
- **Post-Quantum Scenario.** Recent advances in quantum computing threaten the security of the current IoT using traditional cryptographic schemes. We are at the very beginning of the standardization process for quantum resistant algorithms, and research on their application in the IoT is limited. Anticipating the post-quantum scenario in addition to reducing computational requirements may also directly give rise to resistant authentication algorithms in this type of scenarios.

5.9 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.

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 should be a focus in the next few years, as online presence and technologies (such as IoT to everyday scenarios in Smart Cities) are soaring. Special attention should be paid to technologies like blockchain or credentials, which are promising for secure, privacy-aware, and trustworthy identity management. Also, regulations like GDPR and eIDAS are expected to be the key differentiating factors of the sector in 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 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, 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 PSD2¹⁸⁹ (Payment Service Directive 2), the ECB SSM (Six Step Model)¹⁹⁰ (European Central Bank Single Supervisory Mechanism) and the T2¹⁹¹ (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 Guidelines¹⁹² (Guidance on cyber resilience for financial market infrastructures), the financial market infrastructures are introducing their procedures to enhance the 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

¹⁸⁹ Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

¹⁹⁰ <https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html>

¹⁹¹

https://www.ecb.europa.eu/paym/target/target2/profuse/nov_2018/shared/pdf/Information_Guide_fo_TARGET2_use_rs_v12.0.pdf

¹⁹² Guidance on cyber resilience for financial market infrastructures.

<https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf>

e-IDAS¹⁹³ (electronic identification and trust services), GDPR¹⁹⁴ and NISD¹⁹⁵ (Directive on Security of Network and Information Systems see Figure 9), 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.

ENISA¹⁹⁶ 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.

¹⁹³ Regulation (EU) No 910/2014 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

¹⁹⁴ 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)

¹⁹⁵ Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016.

¹⁹⁶ 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)

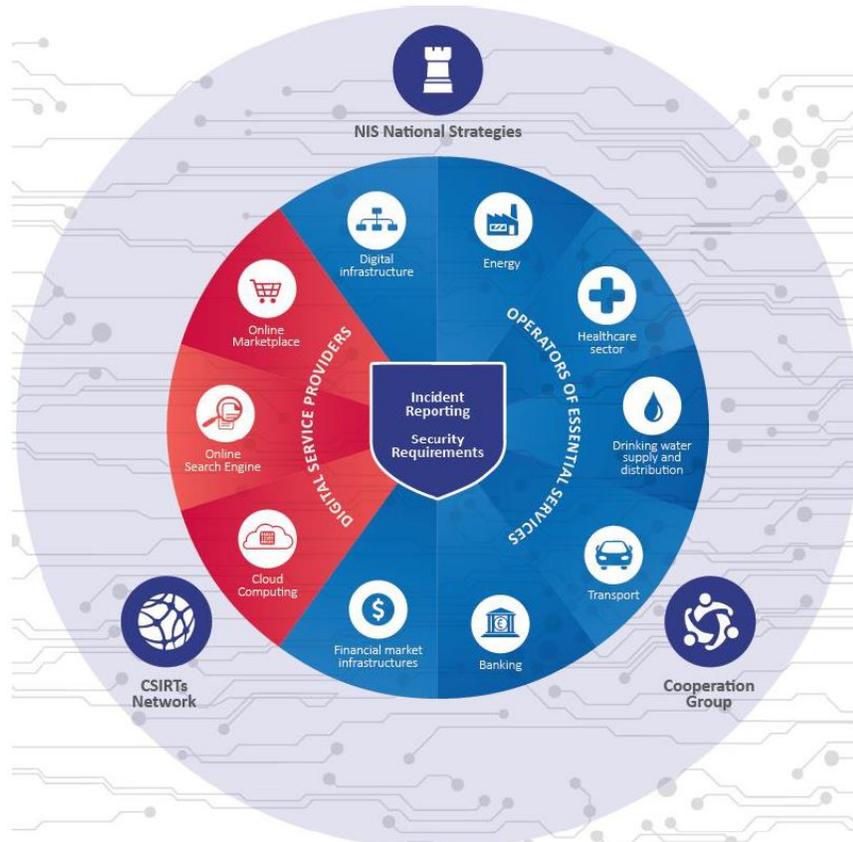


Figure 9: Graphical overview of the NIS Directive. Source: Incident notification for DSPs in the context of the NIS Directive¹⁹⁷

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.

¹⁹⁷ 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>

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 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.¹⁹⁸

It is worth mentioning that in their recent joint advice¹⁹⁹, 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.

¹⁹⁸ EBF position on cyber incident reporting:

<https://www.ebf.eu/wp-content/uploads/2019/10/EBF-position-paper-on-cyber-incident-reporting.pdf>

¹⁹⁹ 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 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:

- 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.

6.5.1 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 [Preuveneers 2020].

6.5.1.1 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 organizations and security managers to be compliant with a specific regulation or to tackle incident management in general. For example, ENISA²⁰⁰ 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 communications²⁰¹, to Supervisory bodies for EU trust services security breach reporting under the eIDAS regulation with a proposal for an incident reporting framework²⁰², and to the Commission and the EU member states with a report containing guidelines on reporting NIS Directive breaches²⁰³. ENISA also offers a visual tool named “CIRAS”²⁰⁴ (Cybersecurity Incident Report and Analysis System), which publishes anonymized 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 Computer Security

²⁰⁰ <https://www.enisa.europa.eu/topics/incident-reporting>

²⁰¹ Technical Guideline on Incident Reporting. Technical guidance on the incident reporting in Article 13 a (Version 2.1, October 2014) ENISA.

²⁰² 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.

²⁰³ Incident notification for DSPs in the context of the NIS Directive. February 27, 2017. ENISA.

²⁰⁴ <https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool>

Incident Handling Guide²⁰⁵, published by the National Institute of Standards and Technology (NIST), or the CREST Cyber Security Incident Response Guide²⁰⁶.

The literature also includes more specific documents for reporting to different national supervisory authorities, such as Cyber Incident Reporting – A Unified Message for Reporting to the Federal Government²⁰⁷, provided by the US Department of Homeland Security, or the Australian Government Information Security Manual²⁰⁸, with information about when it is necessary to report a cyber-security incident, which information to include and the points of contact to do it.

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, for example for Nuclear Facilities [Lee 2017] or to be used in Safety-Critical Systems [Johnson 2015].

J. J. González, in his paper Towards a Cyber Security Reporting System [Gonzalez 2005], already foresaw the need and relevance for providers of security services of having a Cyber Security Reporting System (CSRS), equivalent to an Air Safety Reporting System.

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 QRadar²⁰⁹, Alienvault USM²¹⁰ or Splunk²¹¹ (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: Cyphon²¹², TheHive²¹³, Fast Incident Response

²⁰⁵ Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology. Paul Cichonski, Tom Millar, Tim Grance, Kren Scarfone. August 2012. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>.

²⁰⁶ 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>

²⁰⁷ <https://www.dhs.gov/publication/cyber-incident-reporting-unified-message-reporting-federal-government>

²⁰⁸ 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

²⁰⁹ <https://www.ibm.com/es-es/products/qradar-siem>

²¹⁰ <https://cybersecurity.att.com/products>

²¹¹ https://www.splunk.com/en_us/software/enterprise-security.html

²¹² <https://www.cyphon.io/>

²¹³ <https://thehive-project.org/>

Platform (FIR)²¹⁴, GRR Rapid Response²¹⁵ or Mozilla InvestiGator (MIG)²¹⁶. 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 market for various reasons: it provides integration with MISP and, through Cortex²¹⁷, 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)²¹⁸, osTicket²¹⁹ and Open Technology Real Services²²⁰. 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 Dradis²²¹, MagicTree²²² and Metagoofil²²³. They offer the possibility of generating reports but focused on the testing performed.

6.5.1.2 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

²¹⁴ <https://sectechno.com/fir-fast-incident-response-platform/>

²¹⁵ <https://github.com/google/grr>

²¹⁶ <http://mozilla.github.io/mig/>

²¹⁷ <https://github.com/TheHive-Project/Cortex>

²¹⁸ <https://bestpractical.com/rtir>

²¹⁹ <https://osticket.com>

²²⁰ <https://otrs.com/>

²²¹ <https://dradisframework.com/ce/>

²²² <https://www.gremwell.com/>

²²³ <http://www.edge-security.com/metagoofil.php>

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 [NIST 2006]. 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. 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.

6.5.2 Final Goal

The main objective of the research on this vertical is to improve and simplify the process of collection and mandatory reporting of the information about major security incidents suffered by the financial institutions.

6.5.3 SWOT Analysis



Figure 10: 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 10) when considering a European endeavour to develop and deliver the envisaged result.

6.5.3.1 Strengths

This subsection summarizes our major findings in a SWOT analysis when considering a European endeavour to develop and deliver the envisaged result.

6.5.3.2 Strengths

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.

6.5.3.3 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.

6.5.3.4 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.

6.5.3.5 Threats

This vertical is not easy to harvest. The threats listed below illustrate why.

- **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.

6.5.4 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.

6.5.5 COVID-19 Dimension

During the COVID-19 period, according to Interpol²²⁴, 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 2020, Europol [Europol 2020] states it has followed attacks on organizations that play a key role in the supply chains of major financial institutions, which are

²²⁴<https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19>

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 reports²²⁵ that in the European Money Mule Action (EMMA 6) operation, only a few COVID-19 related cases have been reported.

The Financial Service Information Sharing and Analysis Centre (FS-ISAC) reported that from September 2019 to August 2020 there were a total of 91 ransomware incidents reported by the organization's members [FS-ISAC 2020]. 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 reported²²⁶ 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 ENISA²²⁷ and [Interpol 2020] recommend e.g. that organizations deploy multifactor authentication and implement network segmentation.

In a sectoral analysis report, ENISA²²⁸ 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,

²²⁵ <https://www.europol.europa.eu/newsroom/news/422-arrested-and-4%C2%A0031-money-mules-identified-in-global-crackdown-money-laundering>

²²⁶ <https://www.ncsc.gov.uk/news/ncsc-defends-uk-700-cyber-attack-national-pandemic>

²²⁷ <https://www.enisa.europa.eu/news/enisa-news/securing-smart-infrastructure-in-covid-19-pandemic>

²²⁸ <https://www.enisa.europa.eu/publications/sectoral-thematic-threat-analysis>

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 of its service supplier. As of writing (3rd 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.

6.5.6 Green Dimension

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.

6.5.7 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.

6.5.8 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

6.5.9 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

6.5.10 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

6.6 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.

6.7 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.

6.7.1 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 harmonizing 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 smart 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 to meet this type of need for smart data collection, which is included in Challenge 1 for harmonization of mandatory incident reporting. There are some tools that can help the user of the incident management team to understand the incident severity and its extent for some specific types of cyber incidents as a step to the data collection for the 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 will be analysed

during Roadmap 1 to check if they can support the incident management teams in dealing with Challenge 2 and to which extent. Some examples are Cyphon²²⁹, TheHive²³⁰ or Fast Incident Response (FIR)²³¹.

6.7.2 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 categorize the severity of the incident reported. In WP5, a security incident classification methodology will be analysed that, considering the information collected about the incident and applying the appropriate thresholds and criteria defined under each, identifies the need for mandatory reporting to the competent authorities. However, no tool is currently being developed in WP3 to automatize the evaluation of the algorithms defined using the data collected and the different thresholds and criteria, and to suggest whether there is a need to report for each of the EU regulatory frameworks considered. Nor does there appear to be any open source solution available to address this automatic step of harmonization and facilitation of incident reporting. Consequently, this functionality of the incident reporting platform will need to be postponed also during Roadmap 2.

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. Quantification of the risk can be done 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 should 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 2 this possibility will be analysed.

6.7.3 Incident Reporting

Another consequence of the lack of harmonization (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 of 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 the 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

²²⁹ <https://www.cyphon.io/>

²³⁰ <https://thehive-project.org>

²³¹ <https://github.com/certsocietegenerale/FIR>

communication channels. An incident reporting engine tool will be developed in the context of T3.5 to deal with these challenges.

6.7.4 Collaborative incident sharing platform

In the context of task 3.4 different tools based on the MISP²³² open source threat intelligence platform and open standards for threat information sharing will be 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 will be carried out to improve the security of data exchanged through MISP platform, enhancing and extending its security features, and trust models will be analysed and developed to encourage institutions or organizations 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)	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) and HADES – Automatic analysis of malware samples (D3.1, Section 5.3)	Adaptation of the open source incident management tool TheHive and integration with HADES 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,	Mechanisms to improve trustworthiness and reliability for threat intelligence data sharing using MISP

²³² <https://www.misp-project.org/>

		Reliable-CTIs - Reliable Cyber-Threat intelligence sharing, TIE - Threat Intelligence Integrator (D3.1, Section 5.3)	and qualification of IoCs to improve actionability.
--	--	--	--

6.8 Roadmap

6.8.1 12-month plan

During the first part of the project, we have focused on Challenges 1 and 2, aiming to provide a prototype for an incident reporting platform that helps the incident reporting teams of financial institutions to fulfil the requirements of mandatory incident reporting to the Supervisory Authorities, in particular under the PSD2 and ECB regulatory frameworks.

We have extended the functionalities of TheHive, an open source incident management tool, to support a workflow for mandatory incident reporting in the financial sector under different applicable regulations (using CS4EU²³³ WP3 assets and specific configuration and templates).

During the next 12 months, we plan to start working on Challenge 3, integrating the incident reporting platform through MISP with a threat intelligence sharing platform. Information registered in the incident reporting database will be analysed and shared, and mechanisms will be applied to improve trustworthiness and reliability. Research will be also carried out into the integration of assets in the platform for the qualification of threat intelligence data and the quantification of risks.

Related to Challenges 1 and 2, the plan for next year is to improve the current incident reporting platform prototype by including requirements defined in D5.1 but not yet covered, and the generation of interim and final reports for the currently supported regulatory frameworks PSD2 and ECB. This means that the data collection will need also to be extended to include the additional information required for those reports. We will also try to extend the regulatory frameworks supported.

6.8.2 3-year (or until the end of the project) plan

The plan until the end of the project is to continue consolidating and improving the incident reporting platform regarding these two points:

- extending the number of regulatory frameworks applicable to the financial institutions supported by the platform. In particular, our goal is to include by the end of the project:
 - Personal Data Breach notification under GDPR.
 - Incident Reporting for Operators of Essential Service under the NIS Directive.
 - Incident Reporting for Target2 participants.
 - Incident Reporting for Trust Service Providers under the eIDAS regulation.

²³³ CS4EU: CyberSec4Europe project

Integration in a trustworthy and reliable way with a threat intelligence sharing platform.

6.8.3 Beyond the end of the project plan

Digitalization and an increased connectivity play a pervasive role in society and have become the backbone of the growth of economic sectors, thus increasing cybersecurity risks and making society as a whole more vulnerable to cyber threats. While this demonstrator will only cover the Mandatory Incident Reporting requirements for the financial sector as defined by European regulators, the scope of the need it addresses can be extended to tackle similar challenges across different industries, all of which have the common aim of enhancing the cyber resilience of the Digital Single Market and promoting information sharing across multiple industries and public interest sectors.

The first challenge this demonstrator will address after the lifetime of the project is the extension of its scope of applicability from the mandatory to the voluntary sharing of information on cyber vulnerabilities and threats. Far from being an exclusively technical challenge, notable effort will have to be devoted to building the necessary trust among the entities taking part in the information sharing network.

The second challenge and great opportunity is to deploy such an approach across industries, including both private and public players. This could involve not only the financial sector, but also other sectors that face similar cybersecurity challenges and that could benefit from the knowledge acquired through the experience and the best practices of its users. Indeed, looking at the NIS Directive, finance is only one of several critical sectors that are deemed fundamental for the good function of the Digital Single Market and are recognized as being essential to economic and societal activities.

A third opportunity is to look at widening the geographical scope of the platform, taking into account the jurisdictions beyond the EU borders. While the initial perimeter will be limited to the EU Member States, a further extension to the strategic partners of the EU could also be envisaged.

Additionally, an interesting opportunity is to look into innovative technological solutions to be leveraged in the implementation of the smart incident reporting platform. Since a significant part of the demonstrator's challenge consists in being able to devise secure channels of communication among trusted entities willing to share potentially sensible information, an option could be to appropriately leverage the blockchain technology.

Finally, depending on the outcome of the above-mentioned challenges and on the future developments of EU's cybersecurity regulatory framework, the incident reporting platform could become a valuable data source and may contribute consistently to the general enhancement of the cyber resilience of the Digital Single Market. The information collected through the platform could be especially relevant for the future further development and improvement of the following aspects:

- **Assessment and redress of regulatory gaps and incoherencies.** The existing fragmented implementation of policies and uneven transposition of EU regulations among EU Member States result in legal and operational incoherencies that could threaten the achievement of the overall regulatory objectives. In addition, new gaps and incoherencies will keep emerging as the cybersecurity landscape evolves. In this context, the information collected by the incident report platform could be used to support future relevant developments of the cybersecurity regulatory framework itself. Beyond the lifetime of the project, the platform could (a) provide

- crucial information for the identification of existing and future gaps and incoherencies; (b) enable the development of the appropriate regulation alternatives and adjustments.
- **Assessment of the achievement of policy objectives and development of evidence-based policy.** The information collected by the incident reporting platform could also address the current lack of official data collection on cyber-related matters by EU Member States and enable the future development of evidence-based EU cybersecurity policy. Both the development of evidence-based cybersecurity policies and the assessment of the achievement of the policy's proposed objectives depend on the availability of reliable data and on the definition of appropriate assessment criteria that could arise from the use of the incident report platform.
 - **Assessment and quantification of Operational Risks.** As a further refinement of the development of evidence based policy the ability to provide quantification of risks based on incidents and by using qualifying indicators to estimate the actual impact on one's own infrastructure (see Challenge 3) would bring as a benefit a quantification of a risk area that has been so far mostly qualitative and that could bring significant saving in terms of more precise and optimal assessment and investment in resources. This possibility would strengthen both the individual stakeholders and the overall regulatory regime.
 - **Development of law-making and implementing processes.** Furthermore, the data collected by the incident reporting platform could also assist EU legislators to address the current need for innovative and more flexible procedures regarding the development and the implementation of EU legislation in general, and especially of technology-related regulations. The exponential speed of the development of technologies has already outpaced the EU's ability to design and implement regulations, creating a gap that must be addressed by EU legislators in the near future. In this context, the data collected by the incident report platform could guide the development of new EU law-making and implementing procedures, aiming to guarantee that such procedures are flexible enough to ensure a fit for purpose policy and legislative framework.

6.9 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 6.5.3 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 6.5.4).

We have also analysed how the COVID-19 pandemic has impacted in this vertical (see section 6.5.5) 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 6.5.7), we have identified the following major research areas:

- 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

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 11 and is further explained and analysed in the following sections.

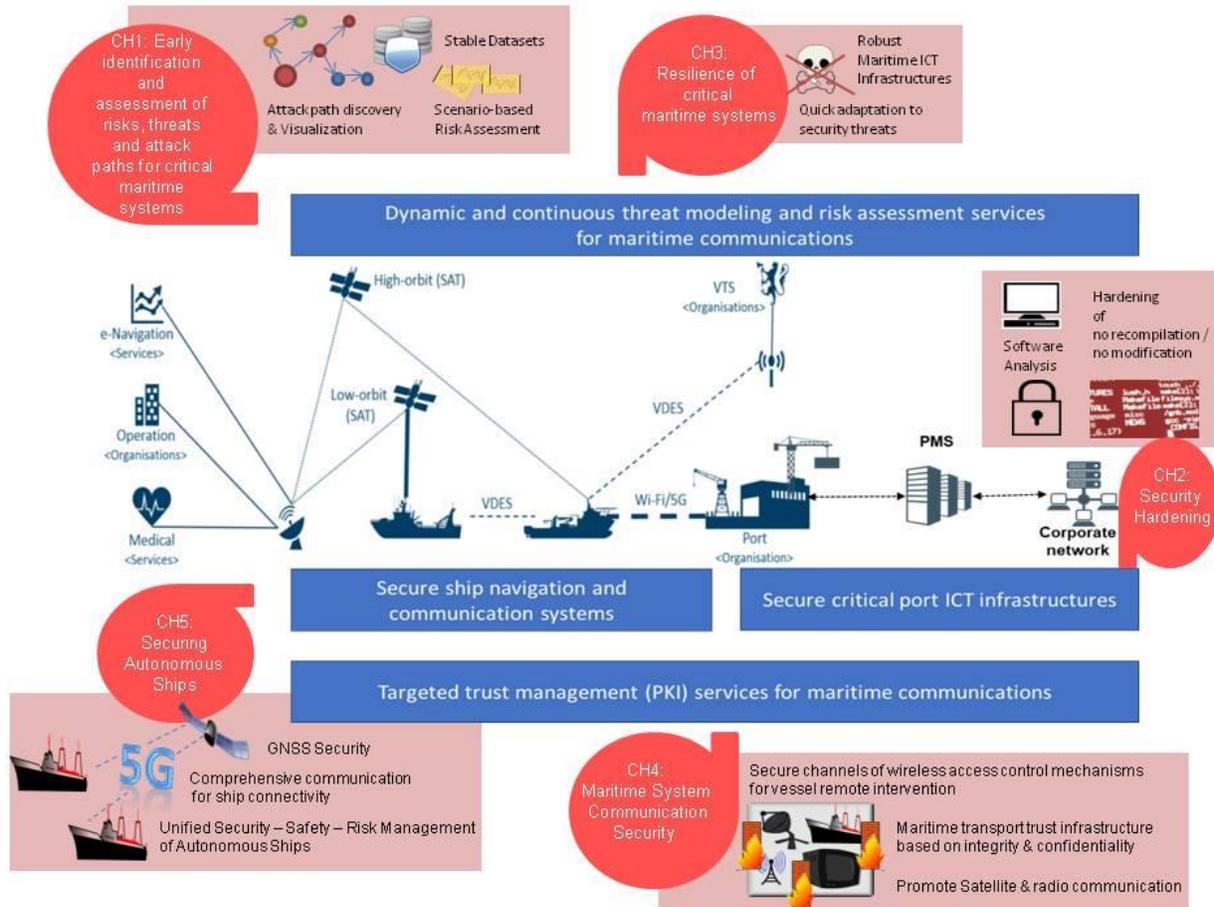


Figure 11: The big picture of a resilient EU maritime transport ecosystem

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 12. 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.

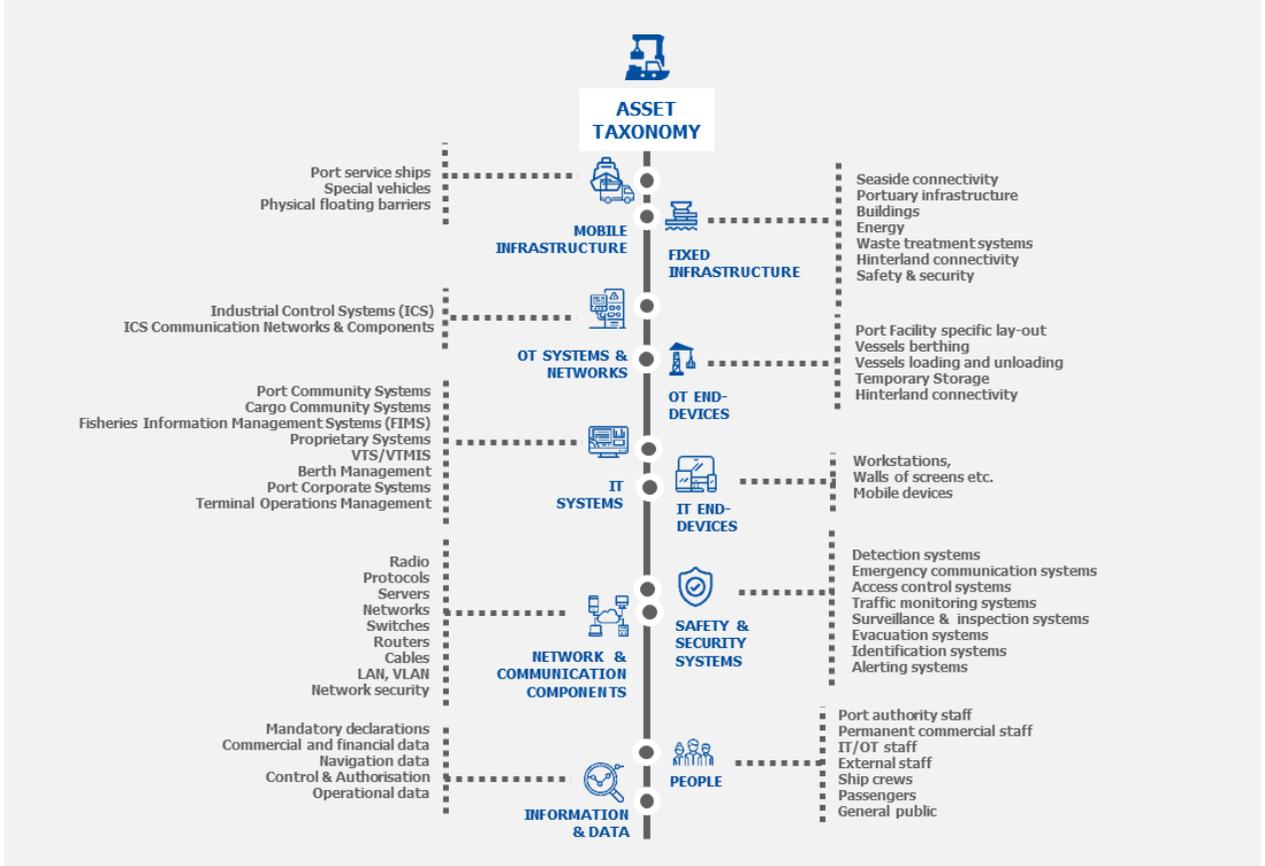


Figure 12: The ENISA taxonomy for critical maritime assets (Source: [ENISA 2019])

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 13. 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 13 [AGK 2019].

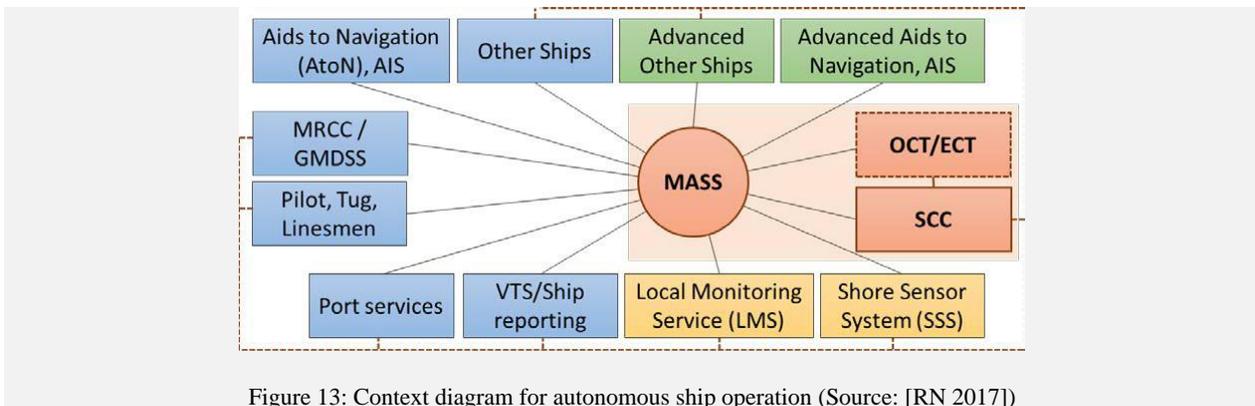


Figure 13: Context diagram for autonomous ship operation (Source: [RN 2017])

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 14:

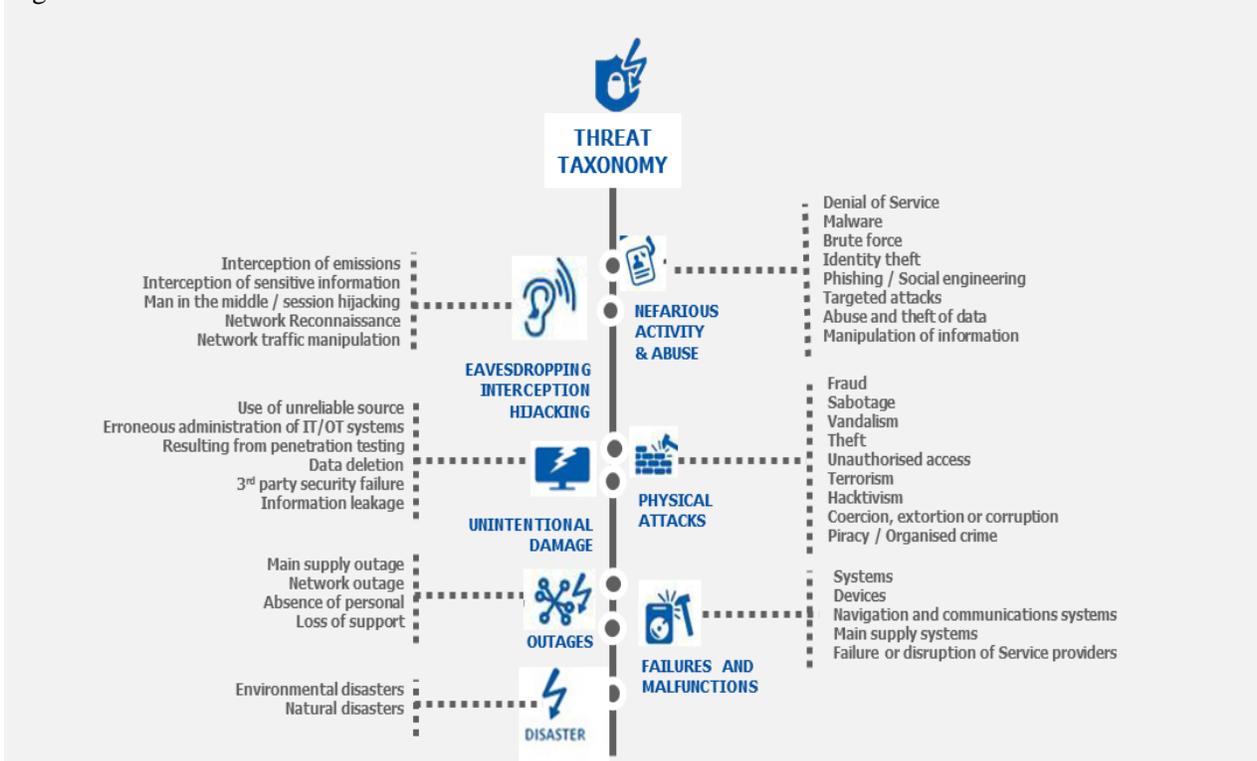


Figure 14: The ENISA threat taxonomy for the maritime transport sector (Source: [ENISA 2019])

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 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.

7.5.1 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 (see section 7.5.8 below). In this section, a research desktop analysis is presented to better capture the state of the art in maritime transport with respect to these research challenges.

7.5.1.1 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. Delegated regulations concerning network and information security, and the protection of critical information infrastructure are the EU NIS Directive [NIS DIRECTIVE 2016], the NIST Framework for improving critical infrastructure cybersecurity [NIST 2018], EU regulation No 881/2019 [EU881, 2019] establishing cybersecurity certification of products, processes and services, and the NIST SP 800-82 guidance on the security of industrial control systems (ICS) [NIST 2015B]. Generic legal frameworks and guidance 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 [ISO/IEC31000 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 [ISO27000 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 [Gagniuć 2017] and Monte Carlo Simulation [Hastings 1970].

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 parts²³⁴, the EVS-EN ISO/IEC 15408-3:2020²³⁵ and EVS-EN-ISO/IEC 18045:2020²³⁶ standards related to the assurance requirements of the IT security evaluation criteria and methodology accordingly: the EN ISO/IEC 19790:2020²³⁷ standard including cryptographic modules and the EN ISO 29134:2020²³⁸ standard on privacy impact assessment. In this line, European Telecommunications Standard Institute (ETSI) sets protocols on advanced networking and risk analysis (ETSI TR187002 2011²³⁹; TVRA ETSI TS 102 165-1 V5.2.3 2017²⁴⁰).

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 2020], the OCTAVE method [Tucker 2020], based on a Bayesian approach using UML, the Magerit [MHAP 2012] open methodology for risk analysis and risk management, and the Mehari method for harmonized risk analysis [CC 2017]. In addition, BowTie [IP Bank 2015] is a primarily qualitative risk analysis method, which 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 the maritime transport, maritime critical infrastructures are vulnerable to various threats and cannot be addressed by traditional risk assessment methodologies [AWW 2017] [Boyson 2014]

7.5.1.1.1 Security law and standards 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 [IMO03] (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 04] (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 [EC84/2002], which reflects the prevention of pollution from

²³⁴ <https://www.iso27001security.com/html/27033.html>

²³⁵ <https://www.evs.ee/en/evs-en-iso-iec-15408-3-2020>

²³⁶ <https://www.evs.ee/en/evs-en-iso-iec-18045-2020>

²³⁷ https://www.cenelec.eu/dyn/www/f?p=104:110:609928853661101:::FSP_ORG_ID,FSP_PROJECT,FSP_LANG_ID:2307986,69303,25

²³⁸ https://www.cenelec.eu/dyn/www/f?p=104:110:1727884474979701:::FSP_ORG_ID,FSP_PROJECT,FSP_LANG_ID:2307986,69257,25

²³⁹ https://www.etsi.org/deliver/etsi_tr/187000_187099/187002/03.01.01_60/tr_187002v030101p.pdf

²⁴⁰ https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/05.02.03_60/ts_10216501v050203p.pdf

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. EU JOIN(2014) 9 applies a security strategy for an open and secure global maritime domain to facilitate a cross-sectoral approach to maritime security.

The IMO Convention on Facilitation of International Maritime Traffic (FAL) has set guidelines for maritime cyber risk management [IMO 2017B]. Maritime security topics are addressed by the ISO 28005-1:2013 standard on security management systems for the supply chain [ISO28005-1 2013], 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 [ISO28007-1 2015] 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 by the end of 2020 plans to publish an updated report on maritime cybersecurity. Moreover, BIMCO has published guidelines on cybersecurity aboard ships [BIMCO 2018]. A growing number of initiatives regarding vulnerabilities of vessel information system that render ships subject to cyberattacks has been identified recently [DNV GL 2015;2016;2019; ABS 2018]. 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.

7.5.1.2 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.

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.

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 [Ezell 2007; 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 MEDUSA²⁴¹ 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 MITIGATE²⁴² 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.

7.5.1.2.1 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 7.5.1.5.

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.

7.5.1.3 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).

²⁴¹ MEDUSA stands for Multi-ordEr Dependency approaches for managing cascading effects in port's global sUpply chain and their integration in riSk Assessment frameworks

²⁴² MITIGATE stands for Multidimensional, IntegraTed, riSk assessment framework and dynamic, collaborative risk manaGement tools for critical information infrAstrucTrurEs

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.

7.5.1.3.1 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).

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 [CPMWBBGWZHC 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.

7.5.1.3.2 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.

7.5.1.3.3 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].

7.5.1.3.4 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.

7.5.1.3.5 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 contain a single memory page, which are then randomly loaded and shared among the processes.

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.

7.5.1.4 Maritime communication system security and trust infrastructures

The state of the art in security, specifically for Maritime Transport communication systems, is as follows.

7.5.1.4.1 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 15, 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.

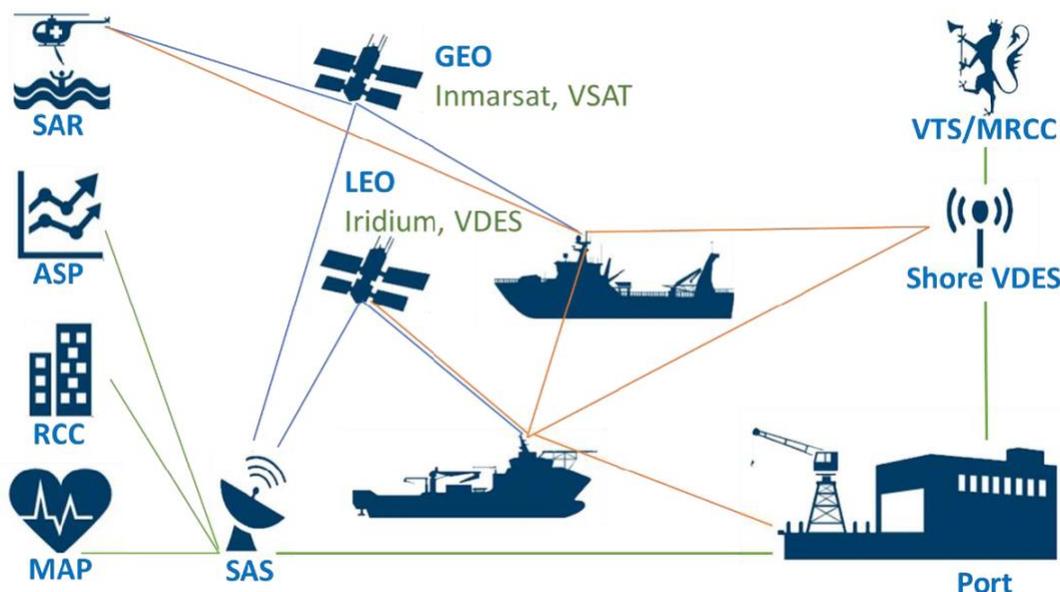


Figure 15. Examples of maritime communication channels

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 16. 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).

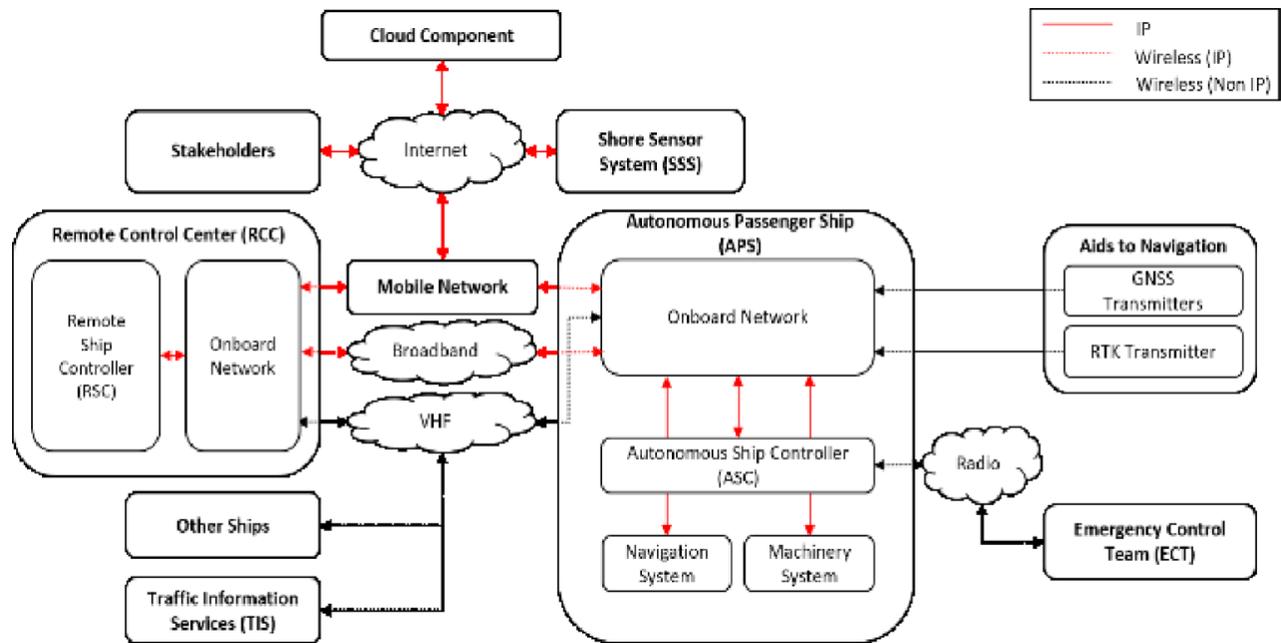


Figure 16: Overview of the APS Context

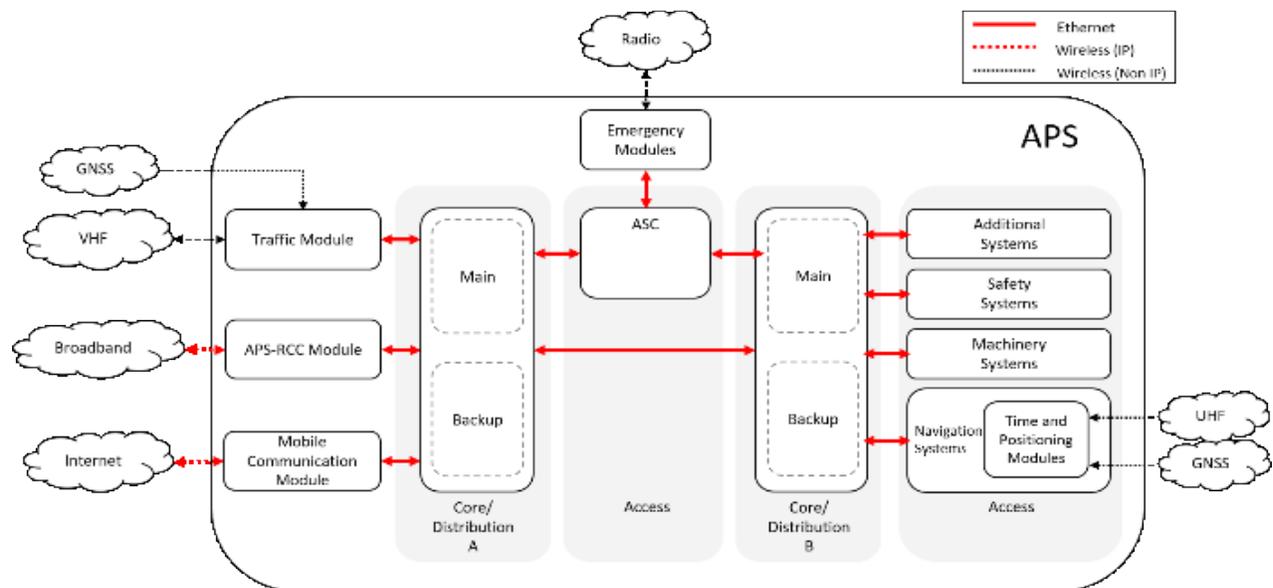


Figure 17: On-board network architecture

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 17. 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.

7.5.1.5 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 (PHA²⁴³) 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.

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

²⁴³ PHA stands for Preliminary Hazard Analysis

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 2020B] proposed a security and safety 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.

7.5.1.6 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.

7.5.2 Final Goal

Investigating methods and setting policies and strategies to ensure the security enablers, namely, confidentiality, integrity, availability, authenticity, accountability, non-repudiation, and reliability of the maritime transport systems, and to increase the sector's situational awareness, will maintain the security of the entire EU maritime transport infrastructure. The provision of cybersecurity awareness in the EU maritime transport sector will raise the maritime transport stakeholders' agility and preparedness against unwanted threat events (including existing and emerging threats, such as advanced persistent threats). This will assist in establishing a resilient maritime transport industry, which could strengthen the EU economy and reinforce EU digital sovereignty.

7.5.3 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 18.



Figure 18: Maritime Transport SWOT Summary

7.5.3.1 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 [DVN GL 2020] has taken over in the maritime transport operations in a highly evolving trend [DVN GL 2020] that increasingly attracts the attention of threat agents (i.e. terrorists, cyberwarriors, political/nation-state adversaries, hackers, 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.).

7.5.3.2 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**

7.5.3.3 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**.

7.5.3.4 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.

7.5.4 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.

7.5.5 COVID-19 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.

7.5.6 Green Dimension

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 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).

7.5.7 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.

7.5.8 Identified Research Challenges in the Maritime Transport Sector

7.5.8.1 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

7.5.8.2 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

7.5.8.3 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

7.5.8.4 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 ITU²⁴⁴ 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.

²⁴⁴ ITU stands for International Telecommunication Union.

- **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.
- **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

7.5.8.5 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

7.6 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).

7.7 Methods, Mechanisms, and Tools

7.7.1 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 7.6.

7.7.2 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].

7.7.3 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] [Sarbinowski et al, 2016] [Clang10]) for critical maritime infrastructures, as described in the relevant challenge (see Section 7.5.8.2).

7.7.4 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.

7.7.5 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

<p>Challenge 1</p>	<p>Early identification and assessment of risks, threats and attack paths for critical maritime systems</p>	<p>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>	<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 CIIs 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>
<p>Challenge 2</p>	<p>Security hardening of maritime infrastructures, including cyber and physical systems</p>	<p>TypeArmor (D5.2, Section 6.2) and VTPin (D5.2, Section 6.2)</p>	<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>
<p>Challenge 3</p>	<p>Resilience of critical maritime systems</p>	<p>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, Section7)</p>	<p>Develop and implement monitoring techniques that will analyse the data, and vulnerability databases providing efficient indexing.</p> <p>Explore, map and address risks related to unwanted maritime security events through the generation of bow-tie diagrams.</p>
<p>Challenge 4</p>	<p>Maritime system communication security</p>	<p>PKI service (CySiMS) (D3.1, Section 7), Secure AIS ASM endpoint (D3.1, Section7) and BowTie Plus (D3.1,</p>	<p>Development of a targeted trust infrastructure. A PKI service provision to support encryption requirements to safeguard data AIS and VDES communication.</p>

		Section 5.2)	
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.

7.8 Roadmap

Based on a deeper consideration of the relevant research challenges for maritime transport cybersecurity identified in the previous version of the roadmap in D4.3 (presented in Section 7.5.8 of the current document), which relies on an extended survey of the existing state-of-the-art methodologies and tools in relation to the identified research challenges, both within and outside the scope of CyberSe4Europe, on the conduction of a SWOT analysis, on the new aspect of the COVID-19 dimension, the green dimension of the current vertical, and how a maritime transport cybersecurity strategy can impact EU digital sovereignty, the following research roadmap has been defined.

7.8.1 12-month plan

Concerning the research challenge described in Section 7.5.8.1(Challenge 1: Early identification and assessment of risks, threats and attack paths for critical maritime systems):

- Achieved goals:* We have already worked on developing **methodologies and tools to procure stable datasets**. Furthermore, an initial consolidated structure of a risk assessment methodology, including threat calculation, vulnerability assessment and threat model identification, has been developed in the context of work for T5.5, based on the MITIGATE methodology. This methodology, along with the respective tools, is capable of providing a method for attack path generation that aims to evaluate the propagation of threat events and to calculate risks to individual and cumulative values. In this respect, visualization techniques have been provided to demonstrate asset network graphs, attack graphs and risk reports, while diagrams are additionally available. At the same time, we have enhanced the existing risk assessment methodology with **evidence-based and scenario-based risk assessment approaches**, based on recent cybersecurity incidents that encapsulate sophisticated attacks and provided supporting threat scenarios to satisfy active learning processes (i.e. problem-based and case-based learning).
- Expected goals:* In our updated 12-month plan, we plan to improve the cyber-attack path discovery algorithms that are capable of capturing the dependencies and interactions of maritime systems. Furthermore, we aim to improve the visualization techniques for illustrating **vulnerable attack paths and attack patterns**.

Concerning the research challenge described in Section 7.5.8.2 (Challenge 2: Security hardening of maritime infrastructures, including cyber and physical systems):

- *Achieved goals:* Regarding system hardening, the initial plan included an analysis of available components for applying the necessary hardening techniques.
- *Expected goals:* In this aspect, we are in the position of having several different hardening techniques for instrumenting various forms of software (source, binary) and for different threats. The mapping of available solutions for instrumenting particular applications to mitigate specific threats will be integrated into the MITIGATE platform. Software hardening tools and solutions will be offered as new controllers in MITIGATE, which will be instantiated for specific threat classes. MITIGATE offers a classification of threats affecting different types of components. Not all threats can be countered using system hardening and not all components can be instrumented for security. Specifically, the plan for integrating all system hardening tools with MITIGATE is as follows:
 - We will enhance MITIGATE with new controllers for software hardening. Controllers are security components that can be effective in countering particular threats.
 - We will map all applications that are affected by threats addressable through hardening. Such threats are memory-corruption attacks, which can be used for exploiting native code.
 - Finally, we will enable the new controllers for the aforementioned threats.

Concerning the research challenge described in Section 7.5.8.4 (Challenge 4: System communication security):

- *Achieved goals:* We have developed the necessary components for a trust infrastructure based on a PKI specifically configured for the limitations found in the maritime domain.
- *Expected goals:* We expect to achieve demonstrable integrations between maritime applications and the trust infrastructure. Furthermore, we seek to implement mechanisms for PKI certificate revocation that support ships in offline states and scale to a realistic number of clients (~100 000 – 200 000). We will implement a VDES-ready maritime communications application that emphasises the integrity, authenticity and privacy of messages.

7.8.2 2-year (or until the end of the project) plan

In the course of the next 2 years the research goals to be achieved are the following:

Concerning the research challenge described in Section 7.5.8.1 (Challenge 1: Early identification and assessment of risks, threats and attack paths for critical maritime systems):

- We plan to experiment with enhancing the developed *cyber-attack path discovery algorithms* with novel machine learning techniques, or other computational models that are capable of capturing more accurately the dependencies and interactions of maritime systems.

Concerning the research challenge described in Section 7.5.8.2 (Challenge 2: Security hardening of maritime infrastructures, including cyber and physical systems):

- The software hardening tools and solutions that will be integrated into the MITIGATE platform as new controllers will be further examined to improve their capacity and eliminate possible bugs or malfunctions.

Concerning the research challenge described in Section 7.5.8.4 (Challenge 4: System communication security):

- In this context we aim to work towards offshore trials and standardization of a **trust infrastructure** that takes into consideration the environmental limitations of the maritime transport sector, such as network availability and communication costs. Since stability of communication is an issue, it is crucial to facilitate the availability and stability of communications solutions. Therefore, solutions need to be scalable and redundant. Within this context, a challenge to be met is to **design and implement maritime systems that utilize 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.

7.8.3 Beyond the end of the project plan

The rest of the identified research challenges are expected to extend the lifetime of the project. In particular:

Concerning the research challenge described in Section 7.5.8.3:

- **Ensuring the robustness of the maritime ICT infrastructures** as well as **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.

Concerning the research challenge described in Section 7.5.8.4 (Challenge 4: System communication security):

- **Integrating** the VDES-ready secure communications application **with the hardware** (VDES devices) once the VDES standard has been finalized and the hardware becomes more available for use.

Concerning the research challenge described in Section 7.5.8.5):

- All the research goals identified under this research challenge are research goals that go beyond the lifetime of the project. However, it is expected that some of these goals will benefit from the advances produced by the other research goals. For example, the long-term goal for **unified security and safety risk management of heterogeneous components in autonomous ships** is expected to benefit from the development of stable data sets for the maritime environment, such as the targeted threat models. The secure **5G and satellite integration for ship connectivity in autonomous ships** will take advantage of the development of secure maritime systems for dual satellite and radio communication needs. The goal for a **comprehensive communication architecture for autonomous ships** as well as the goal for **GNSS security** are expected to benefit from the development of a targeted trust infrastructure.

7.9 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.

A bird's eye view on the state of the art (section 7.5.1) 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 7.5.2). 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 7.5.4).

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 (section 7.5.5) and to respond to the Green Deal (section 7.5.6) environmental requirements 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 7.5.5). Thus, reinforcing security in the e-maritime environment could help to amplify the Europe's strategic autonomy (section 7.5.4).

Taking into account the serious impact of maritime transport to the EU economy, 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, that is 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 most prominent challenges in the maritime transport security are considered (section 7.5.8):

- 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 are mapped to the big picture and methods, mechanism and tools have been proposed to address them (section 7.7). Moreover, promising risk management and threat modelling methodologies for the maritime transport should be able to explore the sector-specific security requirements, and the cascading effects in view of a 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 on maritime infrastructures systems hardening (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 dealt with the adoption of optimal risk models that capture holistically the threat landscape of unmanned vessels (Challenge 5). The accomplishment of all the previous proposals could create a resilient maritime transport environment. Such environment should incorporate a “resilience-by-design” agile system that responds quickly to security incidents, be security-aware of the evolving sectorial threat surface, consider interdependencies among infrastructures and the risk propagation consequences, and deploy 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 year²⁴⁵. 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 Forbes²⁴⁶ more than 2.5 quintillion bytes of data were created each day during 2018; 463 exabytes of data per day are expected in 2025²⁴⁷. Data assets in healthcare domain are growing fast than in other sectors²⁴⁸. 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%²⁴⁹.

²⁴⁵ https://www.dellemc.com/en-tz/collaterals/unauth/briefs-handouts/solutions/h17823_solution_brief_driving_real_clinical_business_outcomes_with_a_modern_it.pdf

²⁴⁶ <https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/>

²⁴⁷ <https://www.raconteur.net/infographics/a-day-in-data>

²⁴⁸ <https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf>

²⁴⁹ <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 firewalls²⁵⁰ [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 (Dawex²⁵¹), 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.

²⁵⁰ <http://www.appliedclinicaltrials.com/how-ehrs-facilitate-clinical-research>

²⁵¹ <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**²⁵².

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 2018²⁵³. According to the 2019 Data Breach Investigations Report performed by Verizon²⁵⁴, 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 others²⁵⁵”, 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 data²⁵⁶. 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.

²⁵² https://www.researchgate.net/publication/234034137_Protecting_Patient_Privacy_when_Sharing_Medical_Data

²⁵³ <https://www.hipaajournal.com/healthcare-data-breach-statistics/>

²⁵⁴ <https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief-emea.pdf>

²⁵⁵ <https://www.ecs-org.eu/documents/publications/5ad7266dc1cba.pdf>

²⁵⁶ <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 authorities²⁵⁷, 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:

²⁵⁷ <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 Nightingale²⁵⁸ has been involved in a “secret transfer of medical history data, which can be accessed by Google staff”²⁵⁹. 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 data²⁶⁰.

8.5 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 regulation²⁶¹ came into force in 2016 and was applied on 25th 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.

8.5.1 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 8.7.1 – 8.5.11), 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 representing large quantities of medical data. To address and/or further the research into solving these

²⁵⁸ <https://www.theatlantic.com/technology/archive/2019/11/google-project-nightingale-all-your-health-data/601999/>

²⁵⁹ <https://www.theguardian.com/technology/2019/nov/12/google-medical-data-project-nightingale-secret-transfer-us-health-information>

²⁶⁰ <https://tinyurl.com/r37vb7o>

²⁶¹ https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

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, 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).

8.5.1.1 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 in Section 0 and partially challenge 3 in Section 8.5.9).

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 OpenId²⁶², SAML²⁶³ and Fido²⁶⁴, have been developed to be used as a baseline for such systems.

A modern approach based on self-sovereign identities²⁶⁵ 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+ 2019] make use of distributed ledger technologies, along with user-centric and

²⁶² <https://openid.net/>

²⁶³ 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

²⁶⁴ <https://fidoalliance.org/fido2/>

²⁶⁵ 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 mandatory²⁶⁶ and is widespread in each country²⁶⁷. 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 years²⁶⁸. Initiatives such as go.eIDAS²⁶⁹ are addressing the use of eID with trust services (signing, timestamp, etc.). Examples such as the CEF²⁷⁰ LEPS²⁷¹ 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)²⁷² 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 transactions²⁷³, 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].

8.5.1.2 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

²⁶⁶ <https://ec.europa.eu/digital-single-market/en/e-identification>

²⁶⁷ <https://ec.europa.eu/digital-single-market/en/eu-trusted-lists>

²⁶⁸ <https://ec.europa.eu/digital-single-market/en/eidas-smes>

²⁶⁹ J. Schwenk, <https://blog.eid.as/welcome-to-the-future-of-trust/> 2019.

²⁷⁰ <https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/2016-eu-ia-0059>

²⁷¹ <http://www.leps-project.eu/>

²⁷² https://www.youtube.com/watch?v=P5xjnWL3Pg0&ab_channel=SSIMeetup

²⁷³ eSSIF-Lab, Working for development, integration and adoption of Self-Sovereign Identities (SSI) technologies.

<https://essif-lab.eu/>

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 models²⁷⁴. For example, k-Anonymity, k-Map, δ -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, β -likeness and δ -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 δ -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 accuracy²⁷⁵. 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, SECRETa, TIAMAT, UTD Anonymization Toolbox, and μ -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 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,

²⁷⁴ <https://arx.deidentifier.org/overview/privacy-criteria/>

²⁷⁵ N. Sartor. Data Anonymization Software – Differences Between Static and Interactive Anonymization, 2019.

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 ABE²⁷⁶, 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 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 cpabe²⁷⁷, libfenc²⁷⁸, and Charm²⁷⁹. Possibly the most relevant new implementation since then (excluding the results from the FENTAC project²⁸⁰, which include Crypto-FE²⁸¹) is the OpenABE library²⁸². A list of additional ABE implementations can be found on GitHub²⁸³.

²⁷⁶ 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>

²⁷⁷ <http://acsc.cs.utexas.edu/cpabe/>

²⁷⁸ <https://code.google.com/archive/p/libfenc/>

²⁷⁹ <http://charm-crypto.io/>

²⁸⁰ <https://fentec.eu/>

²⁸¹ <https://github.com/fentec-project/abe-wrappers>

²⁸² <https://github.com/zeutro/openabe>

²⁸³ <https://github.com/topics/attribute-based-encryption>

8.5.1.3 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 in Section 8.5.10). 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 definitely the GDPR Guidelines, Recommendations, and Best Practices²⁸⁴ 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 most 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)²⁸⁵. The Data Protection Commission of Ireland has issued guidelines²⁸⁶ (they are used as an example, because they are in English and understandable to the readers of this document), as have other EU countries' Data Protection Authorities²⁸⁷, 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 organizations that cannot allocate a considerable amount of resources to performing a DPIA. Existing general tools for performing a DPIA include the DPIA template²⁸⁸ by the ICO of the United Kingdom, the tool²⁸⁹ of the European Union Agency for Cybersecurity (ENISA), and the PIA software²⁹⁰ 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 to specific needs: the Privacy by Design and Data Protection Impact Assessment (DPIA) Toolkit²⁹¹ by Edinburgh Business School, and the Code of Conduct and the DPIA

²⁸⁴ https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

²⁸⁵ <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>

²⁸⁶ <https://www.dataprotection.ie/en/organisations>

²⁸⁷ https://edpb.europa.eu/about-edpb/board/members_en

²⁸⁸ <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/>

²⁸⁹ <https://www.enisa.europa.eu/risk-level-tool/>

²⁹⁰ <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment>

²⁹¹ <https://www.hw.ac.uk/documents/privacy-bydesign-dpia-toolkit.pdf>

template²⁹² 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) tool²⁹³, and the Data Protection Impact Assessment (DPIA) Tool for Practical Use in Companies and Public Administration²⁹⁴.

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].

8.5.2 Final Goal

The main objective of the research work in the Medical Data Exchange demonstrator is to improve the privacy-preserving aspects related to sharing sensitive data such as medical records with third parties. In this regard, when data are anonymized the GDPR regulation does not consider them as personal data. Therefore, marketplaces and organizations involved in data sharing will reduce costs in terms of time and effort when data are anonymized. Additionally, the use of tools assuring end-to-end data protection when the data are in transit benefits data citizens' security and privacy. Moreover, the use of techniques for improving the secure access to the marketplace will increase users' trust in these platforms and their willingness to share this kind of sensitive data. Finally, the strategy of performing some DPIA on the platform and applying GDPR guidelines provided by research activities during the development of the project will help to increase users' trust.

8.5.3 SWOT Analysis

Figure 19 shows the SWOT analysis performed for the medical data exchange demonstrator.

²⁹² <https://iapp.org/resources/article/template-for-data-protection-impact-assessment-dpia/>

²⁹³ <https://localdigital.gov.uk/funded-project/digital-data-protection-impact-assessment-dpia-tool/>

²⁹⁴ <https://www.dsfa.eu/index.php/en/home-en/>



Figure 19: Medical Data Exchange SWOT

8.5.3.1 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.

8.5.3.2 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 data²⁹⁵;
- 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.

8.5.3.3 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 fight worldwide pandemics;
- Support from worldwide policy makers and institutions: European Commission, OMS, WEF²⁹⁶.

8.5.3.4 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 deal²⁹⁷.
- Lack of trust from citizens.

8.5.4 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 developing actions and supporting initiatives that help citizens and companies in Europe achieve this end²⁹⁸. 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 year²⁹⁹), the

²⁹⁵ <https://eudatasharing.eu/fr/node/392>

²⁹⁶ <https://www.covid19-dataexchange.org/resources>

²⁹⁷ <https://www.cnbc.com/2020/06/08/palantir-nhs-covid-19-data.html>

²⁹⁸ [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)

²⁹⁹ https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

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 budget³⁰⁰. 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' sovereignty³⁰¹.

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.

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.

³⁰⁰ https://ec.europa.eu/health/europe_2020_en

³⁰¹ [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)

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.

8.5.5 COVID-19 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.

8.5.5.1 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 Organisation³⁰², 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 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.

³⁰² www.who.int

- 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 website³⁰³

8.5.5.2 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 delivered³⁰⁴ 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 States³⁰⁵

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
Spain	Radar Covid	Yes	Yes

In order to leverage the effort made by the EU Member States, the EC has launched an EU interoperability gateway³⁰⁶ 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

³⁰³ <https://www.covid19-dataexchange.org/resources>

³⁰⁴ https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en

³⁰⁵ <https://www.covid19-dataexchange.org/resources>

³⁰⁶ https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1904

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 States³⁰⁷

	Corona-Warn-App ³⁰⁸	TousAntiCovid ³⁰⁹	Radar Covid app ³¹⁰
Country	Germany (Robert Koch Institute-German national public health institute)	France	Spain
Open source	Yes	Yes	Yes
Third countries	Slovenia (#OstaniZdrav ³¹¹)	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 address telephone number or email, geolocalization, tracking movements.	No	No	No
Personal identity data delivery	No	No	No

³⁰⁷ <https://www.covid19-dataexchange.org/resources>

³⁰⁸ <https://www.coronawarn.app>

³⁰⁹ <https://www.gouvernement.fr/info-coronavirus/tousanticovid>

³¹⁰ <https://radarcovid.gob.es/>

³¹¹ <https://play.google.com/store/apps/details?id=si.gov.ostanizdrav>

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 points³¹²:

- **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 estimation³¹³ (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 report³¹⁴ 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 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.

³¹² <https://www.beckershospitalreview.com/healthcare-information-technology/why-contact-tracing-apps-fail-it-experts-share-5-reasons.html>

³¹³ <https://www.thelocal.com/20200909/do-any-of-europes-coronavirus-phone-apps-actually-work>

³¹⁴ <https://hbr.org/2020/07/how-to-get-people-to-actually-use-contact-tracing-apps>

8.5.6 Sector-specific Dimensions

The exchange of medical data involves several dimensions in the healthcare sector³¹⁵, 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.

8.5.7 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)

³¹⁵ https://publications.jrc.ec.europa.eu/repository/bitstream/JRC111441/taxonomy_final.pdf

- 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

8.5.8 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

8.5.9 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 controversies³¹⁶ 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

8.5.10 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 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

³¹⁶ [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)

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 mandatory³¹⁷. 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.

- **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

³¹⁷ 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. Last accessed 13.11.2019.

JRC Cybersecurity Domain:

- Legal aspects

JRC Sectorial Dimensions:

- Health

JRC Technologies and Use Cases Dimensions:

- Big data

8.5.11 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.

8.6 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 8.5. 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).

8.7 Methods, Mechanisms, and Tools

According to the research challenges described in section 8.5, 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.

8.7.1 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.

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 will be developed in the context of T3.2 during the CyberSec4Europe project.

Data protection tools such as an encryption asset will be used and is described in section 8.7.2.

8.7.2 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.

Crypto-FE “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 FENTEC³¹⁸ EU project and is intended to be used by users providing health data, data providers and data consumers in order to offer end-to-end data privacy.

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

³¹⁸ <http://fentec.eu/>

privacy issues and facilitate the management of risks during data sharing, following the principle of privacy by design.

8.7.3 Challenge 3: Trust mechanisms

As indicated in section 8.5.9, the user willingness to share sensitive data in a DEP (Data Exchange Platform) 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 8.7.1 and 8.7.2 play a crucial role for providing security and privacy during the sensitive data exchange process.

8.7.4 Challenge 4: Regulation accomplish

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 will collect and present in a simple and understandable way the specific points of the GDPR regulation and suggest 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.

8.7.5 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 is currently exploring this topic to decide how to provide its platform with this kind of functionality.

The team performed an in-depth screening of more than hundreds of hours of available solutions (many dozens of those solutions have been laid aside). It appeared that fully automated solutions did not exist – or were far too pricey. Data visualization solutions are indeed more like self-service tools directly used by the end-user or predetermined by data analysts.

Two solutions (Looker³¹⁹ and Board³²⁰) have been deeply analysed and carefully tested. Both products were tested by the team using real data in sandbox environments.

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	SPeIDI (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) Crypto-FE (D3.1, Section 7), PLEAK (D3.1, Section 5.2)	Privacy preserving infrastructure
Challenge 3	Trust mechanisms	SPeIDI (D3.1, Section 5.1), SS-PP IdM (D3.1, Section 5.1) DANS (D3.1, Section 5.1) Crypto-FE (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	Visualization tool developed in the context of T5.6 by Dawex	Graphical representation

8.8 Roadmap

According to the major research challenges detected for the Medical Data Exchange demonstrator and the methods and tools envisaged to be used during the development of the CyberSecurity4Europe project, the planned roadmap to follow until the end of the project and beyond is provided below.

8.8.1 12-month plan

This section provides an update of the developed activities considering the **research challenges** described in section 8.5. The plan during the next 12 months includes the following activities:

Privacy preserving assets. To complete the implementation and operation of the anonymization service (DANS) created for addressing the security and privacy challenges. The DANS asset is offered in two flavours: DANS as a service and as a library. On the one hand, the anonymization can be offered to the data providers by the Covid-19 Data Exchange³²¹ platform as an additional service. On the other, data providers can integrate the DANS library into their own system. These two options facilitate the performance of the anonymization process by the data providers, assuring that data privacy is preserved.

Additionally, initial steps for the use of a DPIA tool have been taken in order so that it can be applied to the data exchange platform during the next 12 months. The first steps for designing Crypto-FE have also been developed.

³¹⁹<https://looker.com/learn/recorded-demo>

³²⁰<https://www.board.com/en>

³²¹<https://www.covid19-dataexchange.org/>

It is expected that the design, implementation and deployment of Crypto-FE asset will be finalized over the next twelve months.

Security tools and trust mechanisms. As planned, initial contacts with France Connect have been made in order to integrate the proxy eIDAS connector (SPeIDI), developed under the CyberSec4Europe project umbrella, with the France Connect system. For the next iteration of the Medical Data Exchange demonstrator, the integration of the exchange platform with the France Connect system through the SPeIDI asset is envisaged. The scope and duration of this integration will be limited, depending on the level of permission the French authority will provide for using the France Connect system.

Regulation accomplished. Initial contacts have been made with UM, the owner of the GDPR guidelines asset.

User experience. In response to the appearance of Sars-Cov-2 in our lives and the spread of the Covid-19 pandemic across the world, Dawex launched the initiative of the Covid-19 exchange platform, which aims to facilitate the work of researchers and health administrations by facilitating data sharing related to the coronavirus dissemination. In this new context, visualization and data assessment tools have been provided. For the next 12 months' period the refinement of these assets will be carried out.

8.8.2 2-year (or until the end of the project) plan

Until the end of the project the plan for addressing the challenges provided in section 8.5 is as follows.

Regarding the **security, trust and privacy** tools included in sections 8.7.1, 8.7.2, and 8.7.3:

- **Finalize the eIDAS network integration** with the Covid-19 Data Exchange platform.
- Perform **the integration of the Crypto-FE asset** for assuring end-to-end encryption between data providers and data consumers.
- **Set the basis for the adoption** (depending on the availability and maturity of assets) of a **decentralized access** to the platform based on the SSI paradigm.
- **Design the activities** to be implemented after the DPIA is performed. In addition, fix any issues that may arise during the integration of the described assets.
- **Provide guidelines** that describe, apart from the use of the assets developed during the project, how the adoption of these assets by data exchange platforms available to data providers and data consumers will increase security, trust and privacy when sensitive data are shared. The lessons learnt during the development of the Medical Data Exchange demonstrator could be extended to other data exchange domains.

Regarding the **regulation challenge** included in section 8.7.4, the envisaged plan described in document D4.3 [Markatos 2020] 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, for use in as many situations and circumstance as possible.

- Additionally, research on regulatory 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 2020]

8.8.3 Beyond the end of the project plan

The proposed activities to be developed after the project ends will be in line with the final results and the lessons learnt during the performance of the Medical Data Exchange demonstrator. The plans provided in D4.3 still apply at this moment, but will be updated depending on the final results of the demonstrator validation [Markatos 2020].

- “Dawex will provide a hybrid data exchange platform, with blockchain capabilities and functionalities for identity management (to be determined in phase 2), the decentralized exchange of data (currently being developed; will not be available for phase 1), and smart contracts (available).
- These hybrid capabilities allow the parties supplying and sourcing the data, as well as the operator of the data exchange platform, to choose between two operating modes for managing the actual transfer of data, and the related payment when transactions are monetized. The decentralized mode takes advantage of the blockchain to allow the exchange to take place without an intermediary, while providing maximum trust, traceability and transparency, addressing the challenges of the healthcare market.
- When considering data exchange, the future of healthcare appears to be implantable medical devices. These are usually very small devices and are consequently limited (in their hardware, and consequently security capabilities). To protect the exchange of data and extend the lifetime of such devices, a new suite of light protocols for authentication, key exchange and possibly even encryption should be designed.” [Markatos 2020]

8.9 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).

Section 8.5.3 depicts an initial SWOT analysis which shows the current situation of the medical data exchange domain in the EU regarding user data sharing while preserving privacy, trustworthiness, security, and complying with regulation. 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 control the pandemic, but as indicated in section 8.5.5 several aspects such as privacy, security, and strategy must be considered in order to reach the expected objectives.

In this context several challenges have been identified in section 8.5:

- Challenge 1: Security tools
- Challenge 2: Privacy-preserving assets
- Challenge 3: Trust mechanisms
- Challenge 4: Regulation accomplish
- Challenge 5: User Experience

Dealing with these challenges should be of high importance in the near future, as an increasing amount 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) return 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 term³²². 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 sovereignty³²³.

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 ensured³²⁴.

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
- Resource Providers - universities, urban planners, think tanks, and technical companies

³²² https://www.eng.it/resources/whitepaper/doc/augmented-city/augmented-city-whitepaper-eng_.pdf

³²³ <https://www.fiware.org/community/smart-cities/>

³²⁴ <https://www.living-in.eu/declaration>

- 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 20):

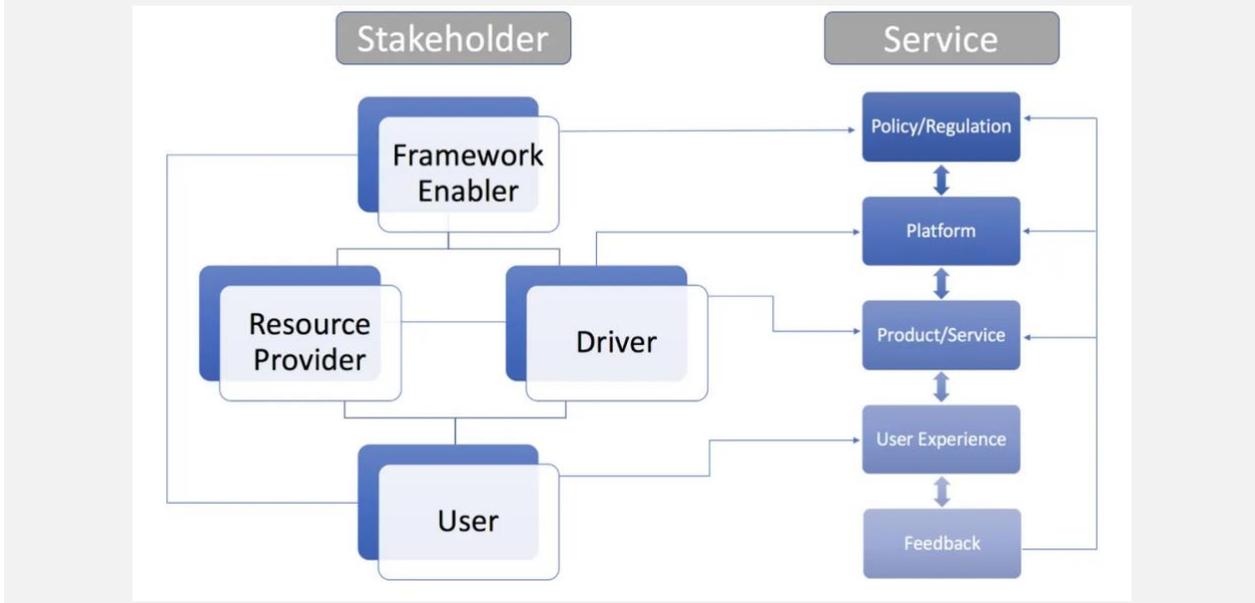


Figure 20: Stakeholders and services

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 SC³²⁵ 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.

³²⁵ SC stands for Smart City

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.

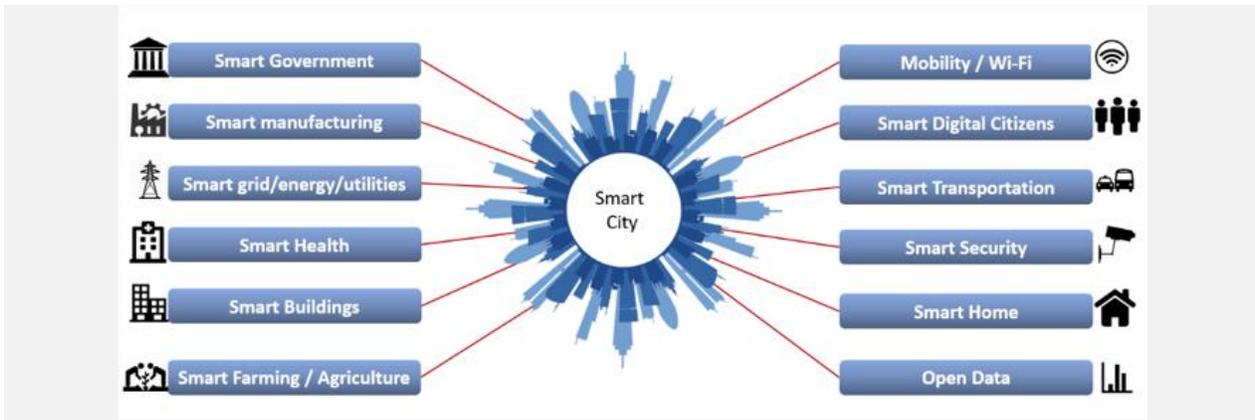


Figure 10: SC Stakeholders (Source: [CER 2019])

ENISA provides several white papers about **good practices for IoT and smart infrastructure tools**³²⁶, 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 21 and Figure 22).

³²⁶<https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool/results#IoT>

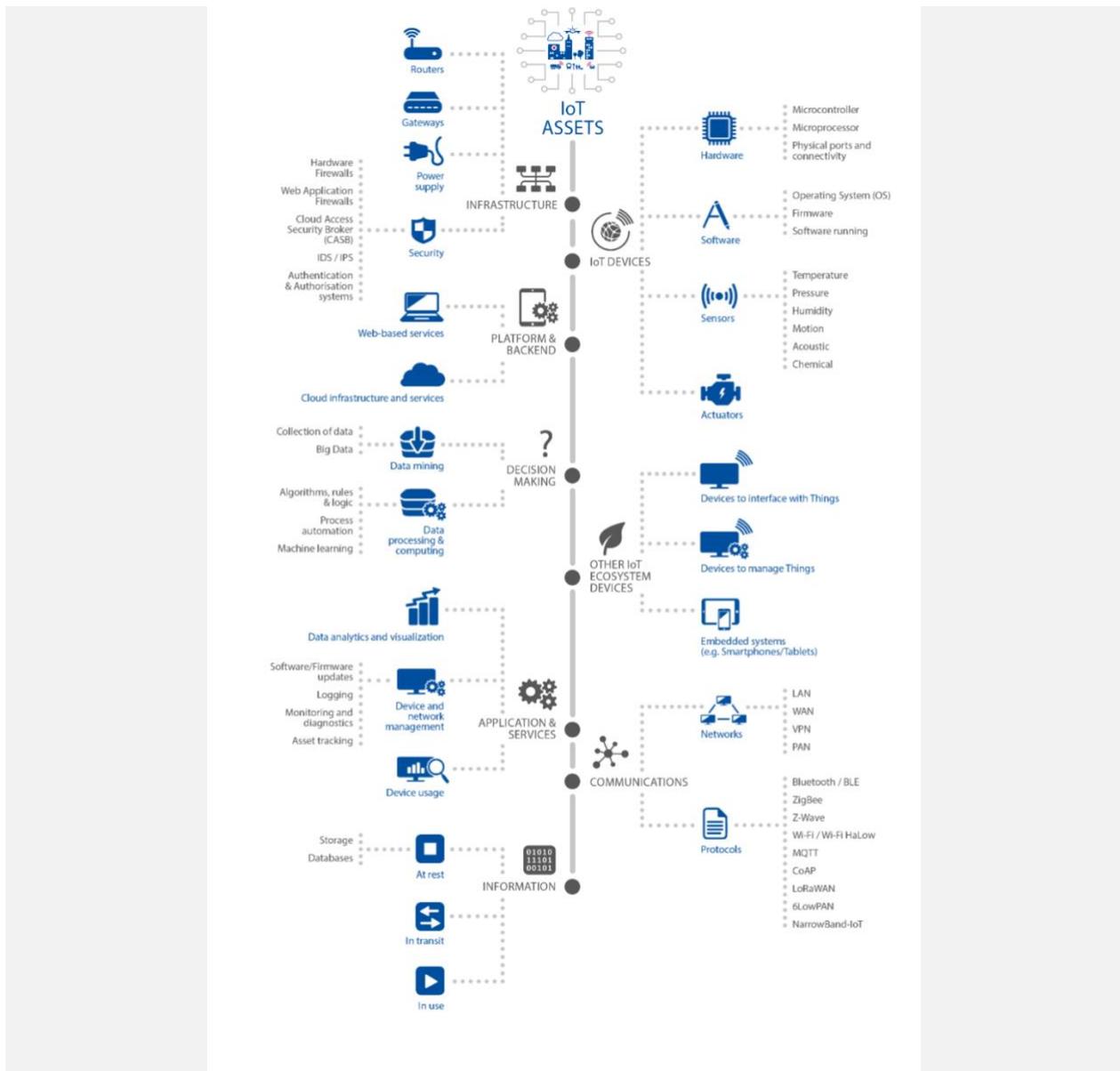


Figure 21: IoT Assembly Taxonomy (Source [ENISA 2018])

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.

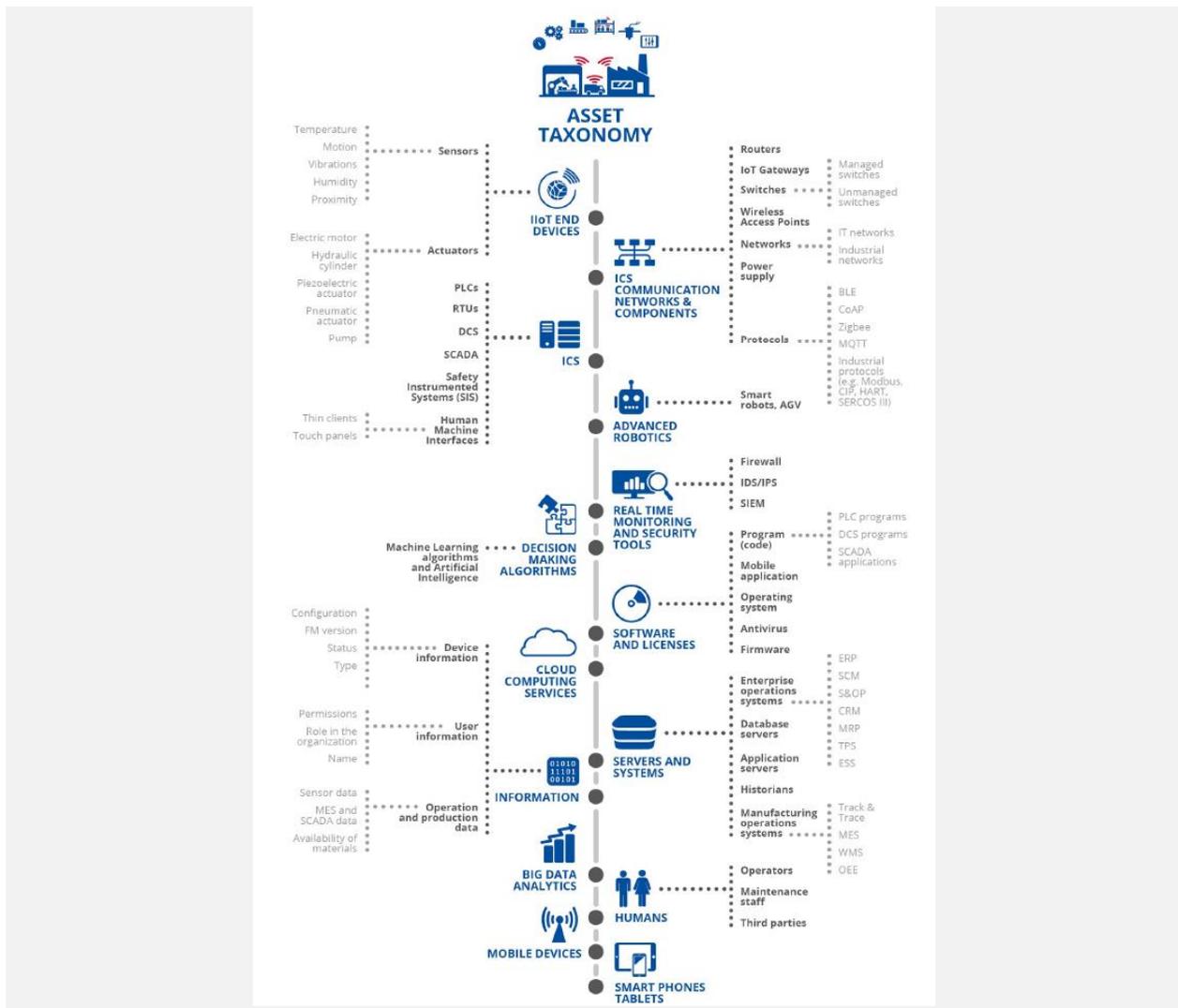


Figure 22: Industry 4.0 Asset Taxonomy (Source: [ENISA 2018])

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 23 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-middle³²⁷: 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.

³²⁷ <https://capec.mitre.org/data/definitions/94.html>

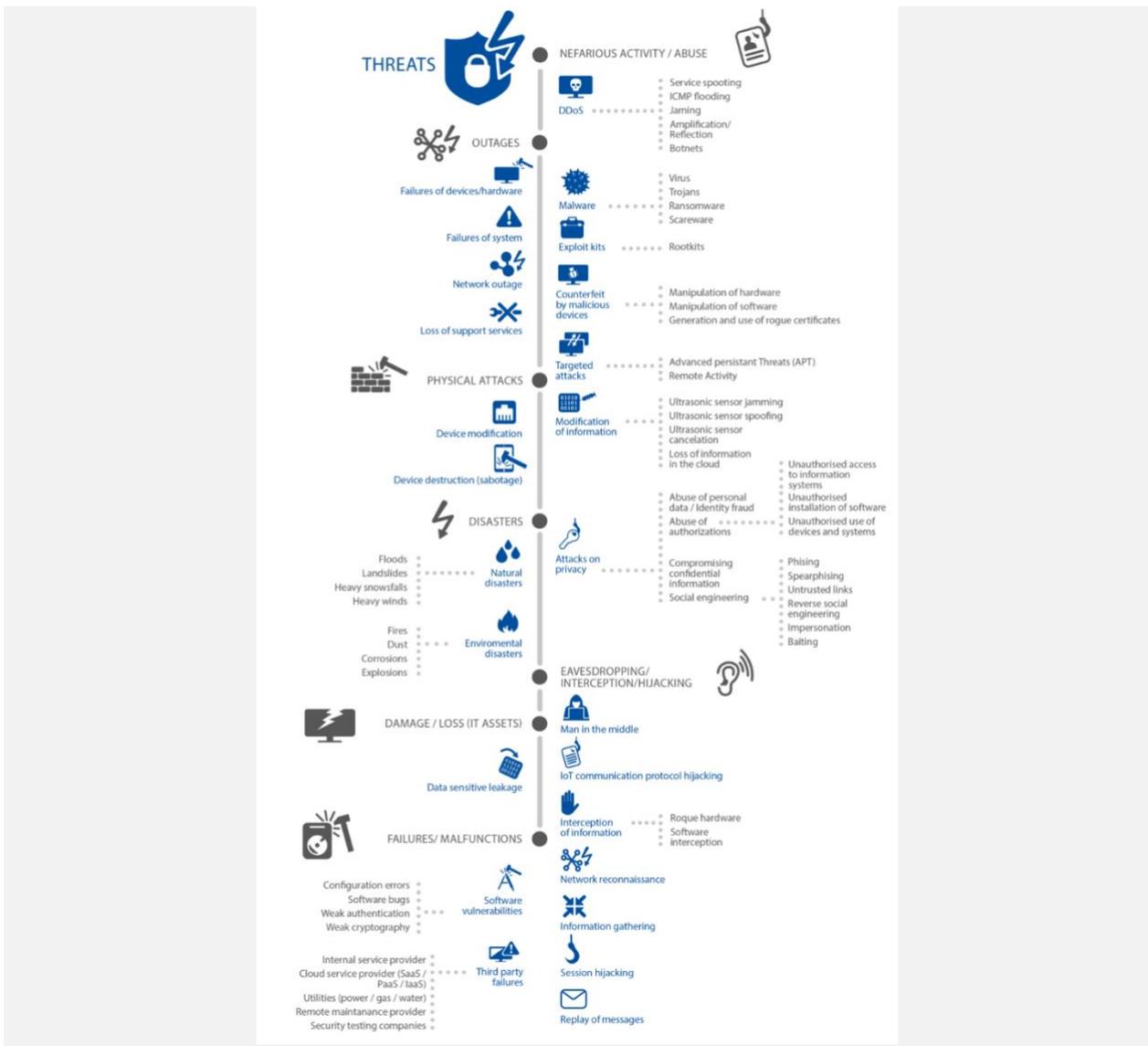


Figure 23: IoT Threat Taxonomy (Source: [ENISA 2018])

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 23, and in Figure 24 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.

Some past attacks on SCs, singled out from among the many, are described below:

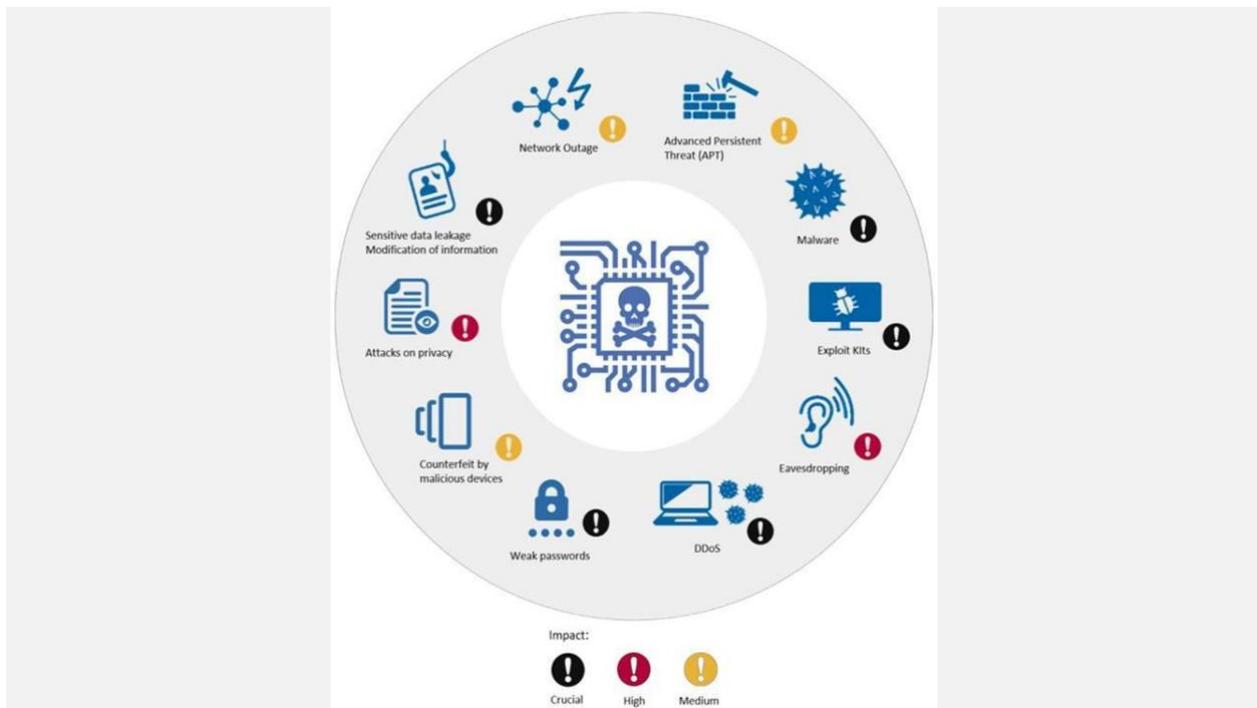


Figure 24: IoT Threats Impact

Ukraine, December 23rd, 2015: attackers compromised energy distribution, leaving 230,000 people without electricity [EISAC 2016].

Sweden, November 4th, 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.³²⁸ On October 11th, 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.³²⁹

San Francisco, November 25th, 2016: municipal railway systems were infected by ransomware [Brewster 2016] and the attackers demanded \$70,000.

Sacramento, November 18th, 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,

³²⁸ https://www.theregister.co.uk/2016/04/12/sweden_suspects_russian_hackers_hit_air_traffic_control/

³²⁹ <https://www.scmagazineuk.com/ddos-attacks-delay-trains-halt-transportation-services-sweden/article/1473963>

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 [KA 2019].

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 [HACKREAD 2019]. 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.

9.4 Who are the attackers?

In such a wide service scenario, Figure 25 lists the threat agents according to the **Intel Threat Agent Library** [Intel 2007] (see Figure 25). 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 25: Intel Threats Identification

9.5 Research Challenges

9.5.1 State of the Art

9.5.1.1 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, it is necessary to consider solutions aimed at enabling the protection of shared data, while still preserving the privacy of data owners, in order to achieve a sustainable realization of SCs. 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 consider the use of the Ciphertext-Policy ABE (CP-ABE) [BSW 2007] to protect confidential data, such as [PRG+ 2020, MEZ 2020, PJB+ 2020]. 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+ 2020] 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 usage 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 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. The Declaration of Cooperation on a European Blockchain Partnership recognises 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.

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.

9.5.1.2 Cyber Risk Assessment

AgID, “Agenzia per l’Italia Digitale” is the Italian agency who has to provide guideline for Italian public administrations (PAs) in their path of digitalization. It is the main point of reference for Italian PAs, Genoa included. With regards to the risk assessment, the Italian agency suggests to “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. It is not doable because this view lacks comprehension about the *peculiarities of the context* and the real *objectives* of a PA³³⁰ (obviously different by a company ones).

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 guideline and standard to learn what is the state of the art in this field and, in the self-assessment phase, the one the project is demonstrating in WP5, the assessment that AgID suggests on the 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.

From EU perspective, the already mentioned ENISA provided a lot of reports and guidelines about the risk assessment and established a specific working group within itself as well.³³¹ 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's 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;
- 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.

³³⁰ PA stands for Public Administration

³³¹ <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/working-group>

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 to use

- 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 on 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.

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 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 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 that uses a number of phases to identify, evaluate and treat risks using the 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, proposes a taxonomy of risk factors and a framework for combining them. 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 Allegro 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 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 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 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.

9.5.1.3 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”(Wikipedia).

A basic bibliography of the old SE school includes (e.g., the ability of D. Mitnick or Frank William Abagnale Jr. to trick humans)³³² [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 due to the involvement of professionals such as psychologists, marketing experts or cognitive scientists in the hacking attacks. The modern Social Engineering 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, have improved a lot in the recent years. Almost all the mainstream security companies are focusing on how the “Human OS” 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 completely changed the landscape in the recent years, are the following two important evolutions:

- The evolution of the social network even through mobile platforms and the corresponding new people’s habits.
- The appearance of some new technologies which allowed to greatly automate most of the SE steps against a large number of people/victims at the same time.

These two factors contributed to the evolution of the social engineering into a new multifaceted phenomenon that it is called Social Engineering 2.0 (SE 2.0), which 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”.

Social Engineering 2.0 is indeed a complex phenomenon that involves several heterogeneous technologies and competences like modern OSINT (Open Source Intelligence): modern SE techniques use data mining

³³² <http://phrack.org/issues/67/15.html>

techniques to cave information from data. The data available on the net is huge. Monitoring of the digital shadow is possible, whilst monitor the digital shadow is not. Information abused for bad purposes is a huge opportunity to improve the efficiency of information gathering in a SE attack.

In the 2020, ENISA published the “ENISA Threat Landscape” about phishing where gives us the numbers 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^{333 334 335}, 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. Although the figure had dropped to 30,8% by the end of 2019, the services mentioned above still remained at the top of the list², with Microsoft 365 services being the phishers’ top target.

Today companies are increasingly doing simulated phishing campaigns to test the vulnerability of their human layer of security. In other words, testing how easily their employees fall for Social Engineering-based attacks delivered by emails (mainly phishing ones). This market was almost inexistent 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 on purpose concentrating on the risk detection functionalities and mainly use the 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”³³⁶. 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 already did), a more comprehensive S.E.L.P. compliance requires

³³³ <https://www.vadesecond.com/en/phishers-favorites-q2-2019/>

³³⁴ https://info.phishlabs.com/hubfs/2018%20PTI%20Report/PhishLabs%20Trend%20Report_2018-digital.pdf

³³⁵ https://docs.apwg.org/reports/apwg_trends_report_q1_2019.pdf

³³⁶ <https://www.gartner.com/en/documents/3950454/magic-quadrant-for-security-awareness-computer-based-tra>

much more work and is considered as a key factor supporting effective EU market penetration. In fact, there is a trade-off between, on one side, the respect of S.E.L.P. principles and regulations and, on the other side, the need to conduct assessments as closer 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 has not a clear picture of the legal and ethical implications of the attack, especially because it is not properly assisted in this by the simulation product, 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.

9.5.2 Final Goal

The SC environment is obviously a complex scenario. It is a system of systems with many different needs from many different perspectives but, as Giulio Cesare said “*Divide et impera*”, the final goal of the research project is to pave the basis for solutions able to address the needs one by one, providing a set of advanced components like Mobile p-ABC (D3.1, Section 5.1), Threat Intelligence Integrator (D3.1, Section 5.3), TO4SEE (D5.2, Section 8.2.3.2), GENERAL_D (D3.1, Section 5.1), PPIIdM (D3.1, Section 5.1), PLEAK (D3.1, Section 5.2), CaPe (D5.2, Section 8.2.3.2), Briareos (D3.1, Section 5.3), RATING (D5.2, Section 8.2.3.2), just to report a few names, that can be easily integrated into SC environment, in order to provide security features, with respect to the protection of end-user data, organizations employees’ account, and infrastructures’ secure access.

9.5.3 SWOT Analysis

Figure 26 provides a summary of the SWOT which is analysed in the sections below.



Figure 26: Smart Cities SWOT Summary

9.5.3.1 Strengths

- Research and proposals and tools specifically conceived for SC systems and their environment will assure strong security and avoidance and/or mitigation of privacy cyber risks at all IoT levels: infrastructure, sensors, service delivery and user applications.
- Thus, the correct and compliant integration between the physical environment, services and digital technologies will be ensured. Additionally, SCs will be protected from the most important cyber-physical vulnerabilities and threats, to assure not only the good functioning of the system itself, but also the avoidance of privacy, data & identity theft, device hijacking, denial of service, application level distributed denial of service, and man-in-the-middle attacks and ransomware.
- The EU has a strong research base in artificial intelligence – for example that of the researchers in the ELLIS society³³⁷ – and many of its applications are relevant to specific SC problems. In a similar way, hardware and software integrity verification has a long history of research, such as the FP7

³³⁷ <https://ellis.eu>

project Secured and the H2020 project Shield, and of industrial success with its application to products and services by Hewlett-Packard and Telefonica. Technologies needed to support these applications are available via European manufacturers, such as Infineon and STM.

9.5.3.2 Weaknesses

The SC concept has been implemented in several and very different ways; hence, there is a great deal of fragmentation that makes it difficult to adopt the same technology in different environments. We lack a common platform of unified services, not because of technological issues, but because of the heterogeneous implementations of various countries and cities.

9.5.3.3 Opportunities

There are opportunities for those concepts and components that provide effective protection and are sufficiently flexible to be easily adopted in different environments. Tools like CaPe, PPIIdM and others, after the demonstration provided by this project, can really change the way we address the challenges depicted below in an operational SC environment.

9.5.3.4 Threats

The biggest threat in the SC environment is to direct research efforts towards a specific city service, without considering the cybersecurity issues that derive from the interoperability among multiple infrastructures in the same network.

9.5.3.5 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”.³³⁸

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]. 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

³³⁸ <https://www.eu2020.de/eu2020-en/eu-digitalisation-technology-sovereignty/2352828>

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

9.5.4 COVID-19 Dimension

COVID-19 has stressed the need for real-time data, personal and non-personal, to be better informed and to improve decision making that can affect society as a whole. The pandemic is fuelling a digital transformation of public authorities, including LPAs. It increases the need for upskilling the work force in utilizing technologies to assess cyber threats and ensure secure sharing of personal and non-personal data. ENG has already a product on the market called Eng-DE4Bios³³⁹, a bio-surveillance platform that enables to monitor the evolution of the epidemic, to map and geolocate infected subjects, and to identify 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 results³⁴⁰.

In the upcoming EU Recovery and Resilience Facility, 20% of the funds will be available to support the digital transition of cities and regions.

The first annual regional and local barometer³⁴¹ provided by the Committee of the Regions, also finds that COVID-19 has stimulated the digital transformation of cities and regions, specifically when it comes to, among others,

- Teleworking
- E-Government
- Communication and Digital Democracy

In particular, the way people access services in indoor environments has dramatically changed during the last year. The countermeasures of the COVID-19 pandemic imposed a disruptive requirement, namely preserving social distance among people in an indoor environment. In this context, CNR is exploring the possibility of adopting indoor localization technologies to measure the distance among 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

³³⁹ <https://www.eng.it/en/our-platforms-solutions/eng-de4bios>

³⁴⁰ <https://www.internationaldataspaces.org/a-biosurveillance-system-for-the-protection-of-citizens-against-covid-19/>

³⁴¹ <https://cor.europa.eu/en/our-work/Pages/EURegionalBarometer-2020.aspx>

exploration of the privacy and trust reputation of an ILS during the discovery phase, and the deployment of the ILS in real-world settings.

9.5.5 Green Dimension

The European Green Deal, an ambitious plan put forward by the European Commission to green the European Economy, is closely linked to SC solutions. In order to achieve the action plan laid out to “boost the efficient use of resources by moving to a clean, circular economy” and to “restore biodiversity and cut pollution” [GREENDEAL], digital solutions using, aggregating and visualizing data from sensors and other sources will become critical for the success of the Green Deal.

Many cities and communities have, in addition to the European Commission’s Green Deal, put forward even more ambitious plans to become climate-neutral by 2025³⁴². The Mission Board for Climate-Neutral & Smart Cities has recently put forward a mission report³⁴³, proposing to make 100 cities in the EU climate-neutral by applying a “radical new way of achieving climate neutrality” – and doing so faster, by 2030. In addition, this report stresses that this highly ambitious goal can only be achieved by leveraging smart systems and data platforms.

This rapid transition requires a cybersecure and trusted environment building on common and open building blocks that can be replicated and scaled across cities and communities in the EU.

9.5.6 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.

³⁴² <https://www.weforum.org/agenda/2019/05/the-copenhagen-effect-how-europe-can-become-heat-efficient/>

³⁴³ <https://euocities.eu/wp-content/uploads/2020/09/2020-09-Cities-Mission-mission-proposal-FINAL.pdf>

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

9.5.7 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;

9.5.8 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;

9.5.9 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);

9.5.10 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);

9.5.11 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);

9.5.12 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 modeling 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
- Defense
- 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);

9.5.13 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);

9.5.14 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
- Defense
- 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);

9.5.15 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
- Defense
- 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 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.

9.7 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"> ● SPeIDI (D3.1, Section 5.1) ● Mobile p-ABC (D3.1, Section 5.1) ● eiDASBrowser (D3.1, Section 5.1) ● DynSmaug (D3.1, Section 5.4) ● VCUCIM (D3.1, Section 5.4) ● EEVEHAC (D3.1, Section 5.5) 	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"> ● Threat Intelligence Integrator (D3.1, Section 5.3) 	Legal Aspects Governance aspects of management, recovery, and continuity Information security
Challenge 3	Cyber competences and awareness program	<ul style="list-style-type: none"> ● TO4SEE (D5.2, Section 8.2.3.2) 	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"> ● GENERAL_D (D3.1, Section 5.1) ● PPIIdM (D3.1, Section 5.1) ● PLEAK (D3.1, Section 5.2) ● CaPe (D5.2, Section 8.2.3.2) 	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"> ● full functionality with full privacy protection; ● privacy protection through the entire lifecycle of the data.
Challenge 5	Cyber response and resilience	<ul style="list-style-type: none"> ● Briareos (D3.1, Section 5.3) ● RATING (D5.2, Section 8.2.3.2) 	Theoretical Foundations Identity Management

Challenge 6	End user trusted data management	<ul style="list-style-type: none"> ● PPIdM (D3.1, Section 5.1) ● DANS (D3.1, Section 5.1) ● PLEAK (D3.1, Section 5.2) ● CaPe (D5.2, Section 8.2.3.2) ● ARGUS (D3.11, Section 5.9) ● PTASC (D3.11, Section 5.8) 	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"> ● SPeIDI (D3.1, Section 5.1) ● PTASC (D3.11, Section 5.8) ● eIDASBrowser (D3.1, Section 5.1) 	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"> ● Briareos (D3.1, Section 5.3) ● RATING (D5.2, Section 8.2.3.2) 	Theoretical Foundations
Challenge 9	Logging and monitoring	<ul style="list-style-type: none"> ● CaPe (D5.2, Section 8.2.3.2) 	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"> ● Mobile p-ABC (D3.1, Section 5.1) ● DynSmaug (D3.1, Section 5.4) ● VCUCIM (D3.1, Section 5.4) ● EEVEHAC (D3.1, Section 5.5) 	Network and Distributed Systems Software and Hardware Security Engineering

9.7.1 Integrated Security Risk Framework

It is 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 COMPACT³⁴⁴ 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.
2. **Do:** Develop and test a potential solution, performing all the actions included in the risk treatment plan.

³⁴⁴ Project co-funded by the European Commission under the Horizon 2020 Programme (GA n. 740712)

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 27) 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.

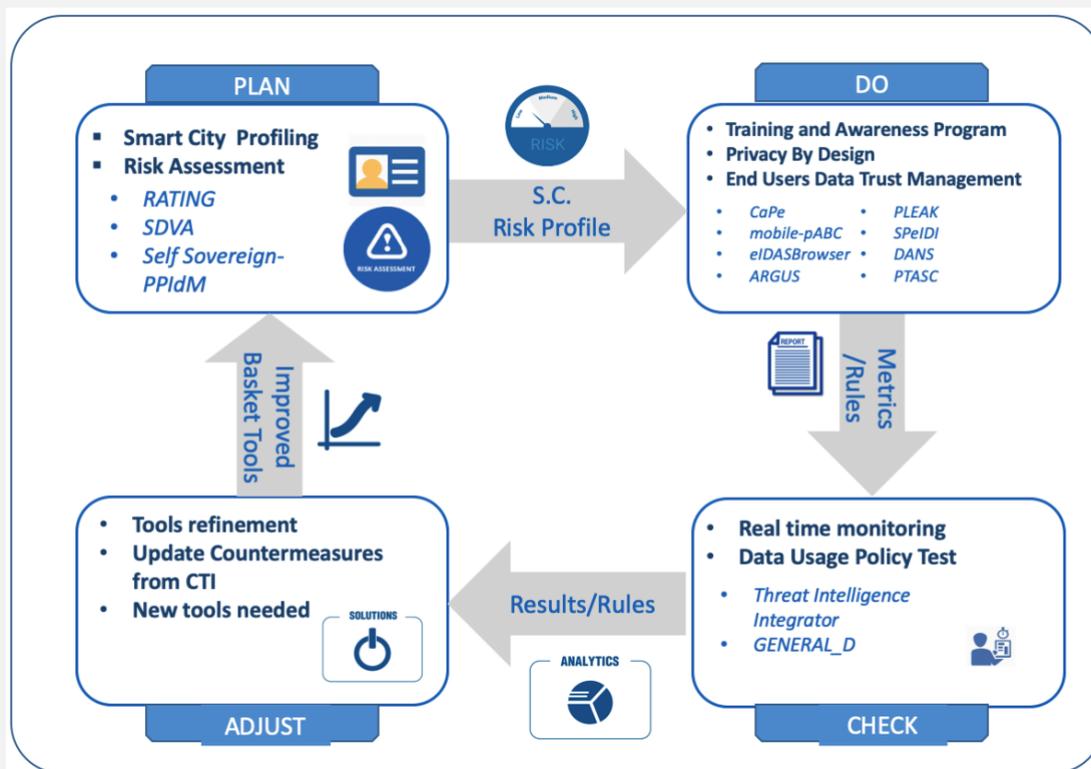


Figure 27: PDCA cycles for SC vertical

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 infrastructure³⁴⁵ (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 guidelines³⁴⁶ 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.

9.7.2 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 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

³⁴⁵ <https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf>

³⁴⁶ <https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing>

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.

9.7.3 Privacy by design and end user trusted data management

Personal data is becoming a new economic “asset class”, a valuable resource for the 21st 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.

9.8 Roadmap

Based on the analysis of the relevant research challenges for SCs identified in section 9.5 and the identified methodologies and tools, the following research roadmap has been defined.

9.8.1 12-month plan

Trusted digital platform. Complete the privacy-preserving authentication and authorization framework by adding range proving and pseudonymity, plus complete integration with the XACML policy management also taking into account specifications from the current privacy regulations, in particular GDPR (e.g., consent management, etc..).

Cyber threat intelligence and analysis platform. For the next 12 months of the project, the SC demonstrator will integrate cyber-threat intelligence and analysis platforms, taking special account of automation and knowledge sharing, in order to increase the effectiveness of defences among stakeholders that share their cyber-threat intelligence. For this purpose, the pilot will integrate an MISP instance that retrieves cyber-threat information from compromised situations. End-users' devices and devices from the pilot infrastructure will gather this information and send it to the MISP instance. Finally, the CTI will share it among other MISP instances from the CS4E project.

Information security and operational security. For the next 12 months, the SC demonstrator will integrate information and operational security within cyber threat intelligence tools. In order to avoid the misuse of information, data will be protected using cryptographic approaches such as CP-ABE, while the privacy of involved entities is still preserved.

Privacy by design and end-user trusted data management. User centric transparency tools will be analysed from a user experience and usability point of view, aiming at a high degree of interoperability with the existing systems of SCs. In the next 12 months, the integration of CaPe (Consent Manager) and GENERAL_D tools for leveraging the SC, with automatic enforcing of GDPR provisions, into executable access control policies will be also finalized. Additionally, testing features will be designed for 1) evaluating the effectiveness of test strategies for the validation of GDPR-based access control policies; 2) testing the GDPR-based access control policies against GDPR requirements; and 3) assessing the GDPR compliance of the access control mechanisms.

Cyber response and resilience The integration of Briareos will allow integrating with TIPS provided by other partners' from the consortium, enhancing the devices' resilience when they are deployed in heterogeneous contexts and scenarios susceptible to attacks.

Interoperability between legacy and new systems. The possible expansion of the user base, thanks to the adoption of the eIDAS regulation, is stimulating LPA to identify in the short term the areas in which investment should be made in the redesign of online systems; in some cases, it will be sufficient to integrate the current legacy authentication systems (for example SIRAC SSO for Genova demonstrator) with eIDAS, while for other systems it will be necessary to proceed with the adaptation of the entire system, including data and internal logic, following the now widespread model of interoperability, in order to allow access to all interested European citizens.

Cyber competence and awareness program. We plan to work, in collaboration with WP6, on providing gamification methodologies and tools to assess and improve cyber competences and cyber-related capabilities for human aspects with respect to phishing attacks. As reported in the last Threat Landscape by

ENISA [ENISA 2020B], phishing attacks represent one of the top 15 cyber threats nowadays; thus, we are moving in the right direction.

Logging and monitoring. We plan to extend the granularity and categories of events in the personal data processing processes that occur among data requestors and data sources (Data Controller and Processors), and data subjects. These events will be collected and managed in a user-centric manner by the CaPe solution. We plan to investigate, in collaboration with WP3 activities, techniques to guarantee non-repudiation and immutability of event logs through the adoption of distributed ledger solutions. In a DLT context, event log metadata may require that personal data and references have to be hashed rather than embedded in the ledger.

9.8.2 2-year (or until the end of the project) plan

Risk assessment. Following the PDCA methodology described in section 9.7.1 (Integrated Security Risk Framework), we will process the DO phase: using the results of the PLAN phase that has just ended, we will perform all the activities needed to resolve the issues that have emerged. The outcomes to be analysed come from the cybersecurity risk assessment tool.

Privacy by design. For the remaining 2 years of the project, specific features will be provided for leveraging SCs with the automatic enforcing of the GDPR provisions within executable access and usage control policies. Additionally, specific features will be conceived in order to: 1) evaluate the effectiveness of test strategies for the validation of GDPR-based access control policies; 2) test the GDPR-based access control policies against GDPR requirements; and 3) assess the GDPR compliance of the access control mechanisms. During the last years, all the provided features will be assembled into a unique framework that can easily be integrated into the SC environment.

Cyber response and resilience. We plan to analyse the results of the first round of penetration testing. We will then perform the activities needed to resolve the issues that have emerged.

Trusted Digital Platform. For the SC demonstration case, we plan to integrate trusted digital platforms tools provided by the partners' consortium. These platforms will provide authentication, user transparency, data protection and data anonymization.

Cyber threat intelligence and analysis platform. For the remaining 2 years of the project, we should be moving towards a mature implementation, taking special account of automation and knowledge sharing, in order to increase the effectiveness of defences among stakeholders that share their cyber-threat intelligence. Finally, during the third year, the full integration should be able to provide a set of defined use cases. Thus, testing will be performed to check and verify the performance of the solution.

Cyber response and resilience. The integration of Briareos will allow integrating with TIPS provided by other partners' from the consortium, enhancing the devices' resilience when deployed in heterogeneous contexts and scenarios susceptible to attacks.

End user trusted data management. As digital identities become increasingly important, it is worth considering how a data management infrastructure can be made more trustworthy, empowering users whilst increasing the availability of data and ensuring citizens' safety and privacy. The plan will examine novel

technologies and cutting-edge ideas in relation to how to build such a trust infrastructure, in particular the development of blockchain privacy-preserving approaches in the context of self-sovereign identity, taking into account aspects related to end-user acceptance and usability. The Porto demonstrator's challenges focus on data processing in a context that presents limited computational, network and storage resources. Aligned with the characteristics discussed, such as interoperability and heterogeneity, these features meet IoT analytics' major challenges. For the remaining 2 years of the project, we will focus on integrating with PTASC to ensure that users can share information without risk, but also allow them to sell the information generated in the SC in a trusted manner. ARGUS will allow devices to connect to a remote server where they can securely control the personal information generated and stored in multiple public cloud providers.

Interoperability between legacy and new systems. In the Porto pilot, PTASC will allow the city demonstrator to have devices to communicate end to end, independently of the architecture. In the Genoa pilot, thanks also to the AGID guidelines³⁴⁷, which strongly push the use of eIDAS to replace SPID level 2 and 3, LPA plan to integrate online services (whose interest also extends to non-Italian citizens) with the new European authentication system, thus giving a new impulse to the economy and social inclusion.

Cyber fault/failure detection and prevention. From the point of view of prevention, the analysis of the cyber-risk self-assessment will offer the opportunity to find out which are the main cyber threats in the SC environment. Our plan is to make them evident to the municipality, highlighting possible mitigation actions to carry out good prevention.

Information security and operational security. To address this challenge, for the next 2 years, it is necessary to continue integrating widely used encryption and access control mechanisms. In the end, the pilot will produce a use case that combines privacy with analysis, exchange and creation of a knowledge database on cyber threats.

9.8.3 Beyond the end of the project plan

It is obviously a complex problem to imagine what will happen after the end of the project, considering the speed with which SCs are evolving today. However, it is reasonable to think that the solutions provided by the CyberSec4Europe project will be taken over by software houses, which will have the task of customizing them and distributing them among their current and potential customers.

Some challenging aspects that can be addressed after the end of the project are:

- **Ensure full participation of stakeholders:** because in the SC environment the most important (and numerous) stakeholders are citizens. To win people's trust and involvement will be a long process, but successful cases like London, Amsterdam and Paris, and the small Reykjavík project [IESE 2019], demonstrate that a real change can be made in people's minds.

³⁴⁷ <https://www.agid.gov.it/en>

- **Adapt governance structures:** this aspect could be affected by the typical resistance to changes in public administration, due to the bureaucratic processes needed to perform any governance innovation. For this reason, it is more realistic to think that it will be a long process.
- **Interoperable solutions:** transporting the IT infrastructure of an LPA into the SC environment involves the adoption of interoperable solutions that are not always already available in the IT assets. It is for this reason that it is necessary to work to make all systems interoperable, starting from those considered strategic, to guarantee a smart service increasingly felt as necessary by citizens who in the SC nourish hope for a new model of life that will also be eco-sustainable. To guarantee all this, it will be necessary for these new IT infrastructures to adopt security requirements more and more intimately, because it becomes essential to guarantee citizens that their digital identity, and therefore also their data in the LPAs, is complete and inviolable. With these bases in the field of IT security it will be possible to build more and more of what is called SC.

9.9 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 9.5.3) 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, (vi) interoperability between legacy and new systems, (vii) cyber competence and awareness, and (viii) in logging and monitoring.

10 Progress since D4.3

In this section we describe the progress that has been made in relation to the 12-month roadmap we described in deliverable D4.3

10.1 Open Banking

The proposal in D4.3 for 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 not yet been resolved: 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:

- a) 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 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.

- b) There is really no great commercial motivation to go through and map out the whole chain. That is really up to more academic/research oriented organisations. 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 eco-system 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 CyberSec4Europe has a strong constituency of academic and corporate partners, the project may be best positioned to progress this topic with a holistic research approach and will be considered as a potential use case for the second cycle of T5.1.

10.2 Supply Chain Security Assurance

In the context of WP5 (D5.1), the main security and privacy requirements that the project needs to address in the supply chain sector were defined through the description of the supply chain use cases and demonstrators. Such demonstrators have been specified in more detail in D5.2, where not only have the use

case workflows been defined and structured, but also various aspects of the 12-month roadmap described in D4.3 have been considered. More specifically, we have used a permissioned blockchain solution in these demonstrators to share supply events between authenticated partners in a secure way. Such events are related to two use cases: i) the resolution of disputes when there are inconsistencies between the order of goods and the received shipment, and ii) providing basic information about the current state of the execution of certain workflows. The use of blockchains for securely sharing information in supply chains can also be found in the recent literature [GKH+ 2020] [WHH 2020], with numerous proofs of concept that are being applied to a variety of supply chains (e.g. food, pharmaceuticals, manufacturing)

Another aspect related to the 12-month roadmap described in D4.3 is the availability of mechanisms and tools for the protection of IT/OT infrastructures and networks. This area has been advancing steadily in the last few years and there have been interesting advances in the last 12 months. For example, advanced hardware-based technologies, such as Physical/physically Unclonable Functions (PUF), are being applied in supply chain scenarios, such as detecting counterfeits using PUF-enabled RFID devices [HCG+ 2020]. In addition, certain certification bodies are exploring the use of vulnerability monitoring services that analyse the security of supply chain IT/OT infrastructures³⁴⁸. Moreover, we have to highlight the integration of big data and AI techniques (including machine-learning and data mining) to manage data and to facilitate decision making [HCG+ 2020] [ABH+ 2020].

10.3 Privacy-preserving identity management

The implementation and deployment of a P-ABC system that meets the requirements of unlinkability and minimum disclosure represents progress, taking advantage of the knowledge acquired in projects such as IDEMIX. Usability and performance are being improved, so that these schemes may be successfully applied in a way that is simple for the end users as well as for the services, encouraging their adoption. Thanks to the knowledge gained in other projects, like OLYMPUS, a new pilot is being considered to improve the use cases depending on whether they are carried out offline or online. OLYMPUS allows the evaluation of other promising to p-ABC approaches, along with other privacy-preserving alternatives that could fit well in our scenarios. In the field of privacy Attribute-Based Credentials (p-ABC), [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. 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.

In this new proposal, there is a work in progress that integrates the OLYMPUS p-ABC's together with the Hyperledger Indy blockchain platform, introducing the advantages of blockchain by providing security and reliability over the operations (issuance, IdP registering...) while maintaining users' privacy.

During the last year, the possibilities of the various cryptographic technologies and available blockchain infrastructures was studied to identify the best possible integration to achieve our objectives. In the same vein, during the first year the authentication system's requirements were thoroughly studied, and the

³⁴⁸ <https://www.intertek.com/cyber-assured/>

system's architecture was designed. Later, a comparison was performed between the different FIDO versions to find the most appropriate based on the current requirements. We concluded that two FIDO versions will be implemented: FIDO UAF and FIDO 2, to expand the system's capabilities to support web authentication.

10.4 Incident Reporting

According to the roadmap proposed in D4.3, a prototype of a platform that helps the incident-reporting teams of financial institutions to fulfil the requirements of mandatory incident reporting is ongoing. The prototype developed so far is in the testing phase, to evaluate its correct operation. This incident-reporting platform is being developed by integrating the assets AIRE (Atos Incident Reporting Engine) and HADES with the open source tool TheHive. We have focused on the generation of the initial mandatory incident report that would need to be sent under the regulatory frameworks PSD2 and ECB. For the collection of all the required information about incidents, the graphical interface provided by TheHive has been integrated into the web interface provided by the AIRE asset. A template has been defined and included in TheHive to be filled in by the user when registering new security incidents in the platform, whereas general information about the financial entities, contacts or regulations (which is shared among different incidents) is completed through the AIRE asset interface. Basic incident impact assessment has been included in the platform through the implementation of a new responder integrated in TheHive³⁴⁹. A basic incident-reporting workflow has been defined for this first phase, and the workflow enforcement is carried out by the AIRE asset through the creation of tasks in TheHive. However, because of the design and constraints of this open source tool in user management, it has not been possible to enforce user permissions on the incidents. The managerial judgement is performed through a questionnaire integrated in the graphical interface. Finally, Excel files are automatically generated and populated with the information collected, following the templates to be sent to the authorities. In this phase one, only those respecting the requirements of ECB and PSD2 regulatory frameworks are included.

10.5 Maritime Transport

In the past 12 months, a requirement analysis of the maritime transport demonstration has been conducted in the context of T5.5 (D5.1). In particular, a set of use-cases were prepared, together with their functional and non-functional requirements (D5.2), enlisting the involving participants (e.g. stakeholders, actors), presenting their step-by-step workflows and recognizing core-functionalities with graphical representations. Within this framework, we have mapped the requirements in each maritime transport use-case. This initial analysis will be the base for the validation of most of the identified requirements, which will rely on both technical and business validation processes, while for some others users/stakeholders will be engaged to some extent in the validation.

As regards the 12-month roadmap proposed in D4.3, during the last 12 months we have worked on developing methodologies and tools to procure stable datasets. To this end, we have elaborated on setting up the respective risk assessment service utilizing the MITIGATE risk assessment tool. In addition, an initial consolidated structure for a risk assessment, including threat calculation, vulnerability assessment, risk

³⁴⁹ A TheHive Responder is a program that reads the information registered about the incident, performs an action and produces a basic result of that action.

estimation and threat model identification, has been carried out in the context of T5.5 work. Further, we have adopted an attack-path generation algorithm to estimate the propagation of threat events and to calculate risks on individual and cumulative values. In this respect, visualization techniques have been provided to demonstrate asset network graphs, attack graphs and risk reports, while diagrams are additionally available. Accordingly, we have worked on evidence-based and scenario-based risk analysis, relying on recent cybersecurity incidents that encapsulate sophisticated attacks, and provide supporting threat scenarios that can be used for active learning processes (i.e. problem-based and case-based learning).

In addition, within these 12 months, we have analysed the available components to apply the necessary security hardening techniques and solutions as new controllers, which will be instantiated for specific threat classes in a later step, which will represent extensive progress on the utilized tool.

Moreover, during the same time period, we have developed the necessary components for a trust infrastructure based on a PKI specifically configured for the limitations found in the maritime domain, to provide an initial setup of the PKI service in a command-line interface.

10.6 Medical Data Exchange

The Medical Data Exchange demonstrator has been affected severely by the Covid-19 pandemic. The already committed end users (hospitals, pharmacies, etc.) have been involved in activities for fighting the spread of coronavirus and also trying to understand and determine the evolution of the pandemic in order to be ready for the emerging new challenges. Therefore, the participation of these actors was compromised. In spite of this big issue, the quick reaction of Dawex (the owner of the data exchange platform) identified this issue as an opportunity for helping to fight the pandemic, launching the Covid-19 Data Exchange platform (a joint initiative by public and private organizations) which facilitates data access and exchange related to the pandemic, with the aim of fighting against the virus and limiting the economic impact. Finally, end-user researchers were engaged to use the platform and the secure, trusted and private data exchange ecosystem created until now in the context of the Medical Data Exchange demonstrator.

The timely implementation of the assets planned during the first 12 months of the project and the quick operation of the new Covid-19 platform allowed us to diminish the initial impact, reducing delays. The rest of the activities planned for this period have been covered without any problem.

10.7 Smart Cities

GENOA: During the last 12 months, the GEN pilot selected the context in which the risk assessment will be conducted. All stakeholders have been identified and the tool environment was set up. Subsequently, the first trial of the tool raised a problem with regard to the financial statement needed to perform the economic loss evaluation. To avoid this issue, we decided to focus the assessment on a specific area related to the “Direzione Sistemi Informativi” division in the qualitative scenario. The assessment was concluded and the results were described in D5.3. The already identified tools for risk assessment, solution elicitation and consent-based personal data management have been finalized and their integration into the SC demonstrators has started. In addition, we are working on the identification and provision of an additional set of tools to protect LPAs from cyber-risks in privacy and security, in order to detect and prevent such attacks, at both individual and organizational level. In addition, we also focused attention on the definition

of a privacy-by-design solution based on Consent Manager (CM) and Access Control (AC), to help organizations comply with the GDPR. The idea is to start from the GDPR text, transform it into a machine-readable format through a given CM, and then convert the obtained outcome to a set of enforceable access control policies (ACPs). We have defined a layered architecture that makes any given system privacy-aware, i.e. systems that are compliant by design with the GDPR. In addition, we have provided a proof of concept by integrating the CaPe and the GENERAL_D proposals. We provided the definition of a possible privacy-by-design architecture, integrating GENERAL_D, an access control manager, and CaPe consent management systems.

MURCIA: The SC “Mi Murcia” Pilot is being developed normally within the roadmap proposed in D4.3. A set of resources to be protected and the way in which we want to interact with them have been identified. An Android application has been introduced that integrates mobile p-ABCs and can perform the authentication processes with eIDAS as well as providing access to the protected resources. The use of OLYMPUS vIdP is proposed to take advantage of the distributed p-ABC and to offer privacy-preserving authentication. At the same time, the use of Keyrock is introduced as a bridge to the eIDAS platform to obtain certified user-related attributes. The pilot provides an SC platform that offers a set of services that include information about public transport, parking status, or real-time information about the use of resources such as water. The introduction of eIDAS provides a trusted platform on which to measure and test in the context of the SC. Mobile p-ABCs provide privacy-by-design, protecting users when using the platform. This system adds the possibility of carrying out possession proofs instead of disclosing everything to the service, increasing user privacy and control over data.

PORTO: During the last 12 months, a risk assessment was performed to understand (i) how personal data is gathered and controlled in the SC, and (ii) how sensor data mechanisms are shared and processed by a third party. In addition, the lab environment was defined based on the FIWARE platform. This allows us to evaluate and scale the demonstrator for Porto’s real-world validation in the future, as well as to study additional security and privacy concerns created by these ecosystems.

11 Related Work

11.1 JRC: Digital Anchor

“Cybersecurity – Our Digital Anchor” is a report of the European Commission that provides a view of the evolution of cybersecurity over the last four decades, identifies weaknesses and challenges in the European landscape, and points to future developments needed for a secure European digital society [BBC+ 2019].

One of the main outcomes of the report is the need for a paradigm shift from the traditional “reactive” discover-patch-evolve strategies to proactive approaches aiming at cybersecurity resilience and security-by-design principles, based on novel ways to deter attacks and to avoid software vulnerabilities, and on consideration of societal needs.

The report focuses on the status and challenges of cybersecurity as

- a core component of societal transformation, in particular in regard to privacy, data protection, trust and finance;
- a vast, multidisciplinary research field with a large landscape in Europe;
- a key component of today’s technology, from big data, to mobile devices, IoT, blockchain, AI and quantum technologies.
- an increasing dimension in societal risks, especially in financially or politically motivated cybercrime, cyberwarfare, and cyberattacks.
- a key aspect to consider in the COVID-19 era: from an increase of cybercrime to disinformation.

The report goes on to identify a set of strategic actions instrumental in building a resilient, secure European digital society, including several “risk mitigation strategies”:

- Deter threat actors through cooperation between law authorities and stake holders, cyber threat intelligence, and knowledge sharing.
- Mitigating vulnerabilities through increased research and innovation, security-by-design and security-by-default approaches to digital products and services, increased education and training efforts, certification and labelling schemes, and vulnerability management methodologies.
- Achieve cyber resilience through rapid incident response and resiliency-by-design methodologies.

and eight areas of action “towards a more secure digital ecosystem”:

- Ethics and rights: cybersecurity must be human-centric.
- Education: high qualification as the only way to correctly implement cybersecurity principles.
- Industry and digital services: involvement of industry to guarantee competitiveness worldwide.
- Research: as the only way to ensure short- and long-term innovation in spite of the rapid evolution of cybersecurity challenges.
- Common culture of collaboration.
- Governance to ensure that cybersecurity is central to policy making.

11.2 Internet Organised Crime Threat Assessment (IOCTA) 2020

The “Internet Organised Crime Threat Assessment” report is a strategic document produced by the European Union Agency for Law Enforcement and Cooperation (Europol) [Europol 2020]. The report aims to analyse the landscape and future of threats related to cybercrime, which is identified as a fundamental feature of the European crime landscape and a particularly challenging one because of its rapidly evolving nature.

The key findings of the report are structured in areas where several emerging and existing-but-increasing threats and challenges are identified:

- Cross-cutting crime facilitators and challenges to criminal investigations: data compromise, cryptocurrencies as facilitators of cybercrime payments and challenges that arise from the tension between the need of law enforcement to access data and data protection.
- Cyber-dependent crime: ransomware, malware, and distributed denial-of-service (DDoS) attacks.
- Child sexual exploitation online: an area that has seen a rapid increase, and where law enforcement is being challenged by the use of stronger encryption mechanisms in criminal activity, the growth of the Darkweb, and the fact that livestream is becoming mainstream.
- Payment fraud: an area that has seen an increase in SIM swapping and SMSing attacks, business email compromises, online investment and card-not-present frauds, and terminal and black box attacks.
- The criminal abuse of the Darkweb: a marketplace that is seeing rapid developments, where criminals use alternative markets as others are secured, and where emerging techniques such as privacy enhancing wallets pose challenges to law enforcement forces.

The report also identifies a set of recommendations

- More and better coordination and cooperation between public and private sectors across borders, in particular between hosting services, social media platforms and ISPs.
- Increased and more efficient information sharing mechanisms as a crucial way to achieve a timely response to cybercrime.
- Prevention and awareness as vaccine against the fact that cybercrime often exploits a lack of basic cybersecurity hygiene and understanding, as well as better crisis management and emergency response mechanisms.
- Enhancement of the legal framework, in particular to better align international and national laws and legislation with cybercrime investigation practices.
- Capacity building among law enforcement forces to counterbalance the increasing skills of cyber criminals.

11.3 Strategic Foresight Report 2020

The 2020 Strategic Foresight report “Chartering the course towards a more resilient Europe” provides a vision to strengthen the resilience of the EU in several interrelated areas: society, economy, geopolitics,

sustainability and digitalisation³⁵⁰. Policymakers are the report's main target. The report analyses weaknesses, strengths and possibilities for the EU's resilience in those areas and suggest a reconsideration of megatrends and long-term plans, in particular with regard to wellbeing, job and labour markets, capacity building, value and supply chains, democracy, trading, emerging technologies, and green and digital transitions. Indeed, the report envisions resilience in all policy areas as a necessity to support the green and digital transitions and the achievement of the United Nations sustainability goals, while keeping the vision of the EU and strengthening its leading role in difficult and rapidly changing times.

The report does not focus on cybersecurity, but on rather on broader aspects of Europe's capacities and vulnerabilities in the mentioned areas. Cybersecurity vulnerabilities and cyber components in hybrid (cyberattacks, cybercrimes) are identified as one of the main concerns in relation to critical infrastructures (health and finance) and democratic systems. In addition, the EU security environment, including, the cyber component, is mentioned. The report also indicates the importance of digital resilience and the leading role of Europe, as a leader of international standards on privacy and data protection, as one of its strengths and thus as a basis for future leading and collaboration opportunities.

11.4 Cyberwatching.eu EU Cybersecurity & Privacy Interim Roadmap

The document "D4.4 EU Cybersecurity & Privacy Interim Roadmap" [Miller 2020] provides a summary and overview of the EU project Cyberwatching.EU, enriched with a preliminary roadmap that the project will further develop in a forthcoming dedicated deliverable.

The roadmap starts by presenting a summary of existing roadmaps: ECSO's Strategic Research and Innovation Agenda, the roadmap agenda of Project CAMINO, SecUnity, NIST's framework, and ENISA's "Looking into the Crystal Ball".

The roadmap then identifies a set of key areas on which the project believes focus should be placed:

- Cybersecurity by design, in particular including security-by-design and privacy-by-design.
- Training – Education – Raising awareness, with a focus on the fundamental role that the EU Cybersecurity Network and Competence Center can play in this regard.
- Standardization and privacy, as a rapidly evolving field making Europe a leader in cybersecurity and privacy, with several established standards and more in the pipeline, and legislation that does not always enforce those standards (whose adoption thus becomes voluntary).
- International Dialogue, as a key instrument to address the challenges of globalization of infrastructures, services, products, and markets, including cross-border legislation and standards, and privacy and data security at the global scale.
- Establishment of an EU certification scheme as the key instrument to build trustworthy services, products, and infrastructures.

³⁵⁰ https://ec.europa.eu/info/strategy/priorities-2019-2024/new-push-european-democracy/strategic-foresight/2020-strategic-foresight-report_en

In addition, the roadmap identifies three key challenges in emerging technologies:

- Internet of Things, with a focus on the challenge of introducing financial and legal incentives to produce secure devices, while providing flexible instruments adaptable to the extreme heterogeneity of devices.
- Next-Generation Virtualized Infrastructures, such as cloud, edge and software defined networks, which, catalysed by the x-as-service paradigm, are making it easier to build larger and larger systems and services, while at the same time reducing the cost of attacks and augmenting their impact.
- Artificial Intelligence, whose great potential comes with serious concerns and challenges related to privacy, predictability, and comprehensibility.

11.5 SPARTA Roadmap

SPARTA (Strategic programs for advanced research and technology in Europe) is one of the 4 pilots for the forthcoming European Cybersecurity Competence Centre and Network. One of the activities of SPARTA is the identification of challenges in the area of cybersecurity, published as a series of roadmap deliverables (currently at version 1.0). The SPARTA roadmap [Jensen 2020] identifies a set of main challenges, called “SPARTA Program challenges”, as well as additional transversal ones, and so-called “emerging challenges”, i.e. challenges likely to become relevant in the future. More specifically, the SPARTA challenges with their goals and milestones are summarized in the figure below (borrowed from the SPARTA roadmap).

The SPARTA roadmap relies on the JRC taxonomy. This taxonomy was first used in the analysis of previous national and European roadmaps to identify gaps in research domains, technologies and sectors. Such analysis was taken into account in the identification of the challenges of the SPARTA roadmap to try to fill the gaps, notably in aspects addressed by CS4E, such as the research domains “theoretical foundations” and “identity and access management”, and the sectors “maritime” and “supply chain”.

The SPARTA roadmap is itself analysed against the JRC taxonomy to show that how research domains, technologies and sectors are considered in each of the SPARTA challenges. Notably, the SPARTA roadmap challenges do not cover the JRC research domains “Security Management and Governance”, or the JRC technologies “Pervasive Systems”, “Quantum Technologies” and “Satellite Systems and Applications”. All other JRC research domains, technologies and sectors are covered by at least one of the SPARTA challenges, with different degrees of coverage.

11.6 ENISA Report on AI Cybersecurity Challenges

Due to its potential on intelligent and automated decision-making across a span of scenarios and verticals, the significance and impact of AI in society cannot be overstated. Yet AI may expose individuals and organizations to new, and sometimes unpredictable, risks. It may also open new avenues in attacks and methods, as well as creating new data protection challenges. For these reasons, ENISA developed a report on AI cybersecurity challenges [ENISA 2020F], whose main goals are i) the identification, analysis and correlation of assets and assets owners within the AI landscape; ii) the identification of threats and vulnerabilities that can be mapped against such assets; and iii) the description of a set of attack scenarios / failure modes pertaining to core AI lifecycle stages. Note, however, that this report strictly focuses on AI

security (specifically, Cybersecurity for AI), and do not addresses in any way data protection requirements and / or aspects of GDPR compliance in AI systems.

To perform this analysis, the report makes use of a *lifecycle functional view* of typical AI systems. This functional view highlights that data is one of the most important assets of AI, as it is being continuously transformed. The report also identifies the most important *actors* that are actively engaged in these processes, such as AI designers / application designers / developers, data scientists / engineers / owners / brokers, model providers, third-party hardware / infrastructure / software providers, and users.

The report then lists the *existing assets*, classified in 6 categories: processes (data-centric processes and AI model processes), environment/tools (communication systems, data platforms, computational platforms, machine learning platforms, and other tools), artefacts (in terms of security, business, policies, parameters, designs, schemas...), models (algorithms, parameters...), actors / stakeholders (described above), and data (raw data to processed data in various degrees).

Finally, the report provides a detailed threat taxonomy divided in 8 categories, alongside a) a detailed mapping of the *AI assets* to the *AI lifecycle stages*, plus b) another mapping of the *threats* to the *AI lifecycle stages*. All 8 categories, plus a summary of the most unconventional threats, is listed here:

- *Nefarious activity / abuse*: Poisoning data sets and models, misclassification based on adversarial examples, reduce effectiveness of AI ML results.
- *Physical attack*: Model sabotage.
- *Disaster*: Environmental phenomena (heating, cooling, climate change).
- *Failures / Malfunctions*: Compromising AI application viability, performance degradation, 3rd party provider failure.
- *Eavesdropping / Interception / Hijacking*: Data inference / theft, model disclosure.
- *Legal*: Lack of data governance policies, compromising privacy, vendor lock-in.
- *Outages*: Infrastructure / communication outages.
- *Unintentional Damages / Accidental*: Compromising data and model integrity and operations, erroneous configuration.

11.7 ENISA Threat Landscape 2020

11.7.1 Overview

The threat landscape of the European Union Agency for Cybersecurity (ENISA) is identifying and evaluating the top cyber threats for the period January 2019 - April 2020 [ENISA 2020B]. The landscape is divided into 22 different reports. It is structured into two main categories: strategic and technical reports. The content of the 22 reports is based on information available from open sources, such as news media articles, expert opinion, intelligence reports, incident analysis and security research reports. Those resources were used in the first part, where a deep theoretical, in-desk search was conducted on the available literature. The second step was to conduct interviews with members of the ETL stakeholders group who are experts in the field and members of the EU Cyber Threat Intelligence Community. The interviews helped to define

the top 15 threats and validate the initial assumptions. Consequently, the methodology approach that was used is defined as two-pronged, because it consisted of two main steps.

11.7.2 What has changed?

There are significant changes from the threat landscape of 2019 and there are two main reasons for those changes. Firstly, the coronavirus disease (COVID-19) pandemic, which forced the large-scale adoption of technology in many critical contexts, such as health services. In addition, because of the international response for the limitation of viral spread, people shifted to teleworking, distance learning, interpersonal communication and teleconferencing. Furthermore, the COVID-19 pandemic showed that malicious actors had a level of capability that allowed them to adapt to this transformation quickly. Subsequently, the second cause was the continuously increasing trend in the advanced adversary capabilities of threat actors. However, at the same time the IT professionals had to respond quickly to the challenges posed by working/studying from home and ensure security. Thus, cybersecurity has been both the challenge and the opportunity for this transformation.

11.7.3 Recommendations

A major recommendation from ENISA aiming to mitigate cyber threat incidents and their impact is that policy makers and cybersecurity experts should work together to develop a common approach. Moreover, the EU cybersecurity policies have to be revised in order to become more mature and able to depict the technological improvement and the rapid expansion of cyberspace. In addition, the European Union should continue investing in cybersecurity research, with an emphasis on long-term and high-risk initiatives. However, the research in cybersecurity should be multidisciplinary. Given the rapid growth of AI and ML the last decade, their use within CTI could be considered. In conclusion, a tactic that will facilitate knowledge transfer will be the use of open-source CTI material.

11.7.4 Top 15 Threats

Table 11 presents the top 15 threats identified as well as possible mitigations and proposed solutions.

Table 11: Top 15 threats identified by ENISA

Threat	Remarks	Mitigation/ Proposed actions
Malware	<ul style="list-style-type: none"> → Emotet, a banking trojan, was the most prevalent malware strain in 2019 and is evolving in 2020 since it has now transformed to a botnet. → 13% increase in malware targeting businesses was observed in services, education and retail. → Malware-as-a-Service (MaaS) was recorded in the wild. → Additionally to traditional phishing, mobile applications designed to steal payment data, credentials and funds from 	<ul style="list-style-type: none"> a. Implement malware detection for all inbound/outbound channels. b. Inspect the SSL/TLS traffic at the firewall level. c. Establish interfaces between malware detection functions and security incident management. d. Share malware-analysis data. e. Employ mail filtering (or spam filtering) for malicious e-mails and remove executable attachments. f. Regularly monitor the results of antivirus tests.

	<p>victims' bank accounts increased by 50% in the first half of 2019. → Fileless malware attacks increased by 265% during the first half of 2019.</p>	<p>g. Disable or reduce access to PowerShell functions.</p>
Web-based attacks	<p>→ Web is used as a message platform for malware. E.g. malware connects to a Slack workspace messaging service to send the command results, which were delivered through a GitHub Gist snippet in which potentially the attacker was adding commands. → Widespread malvertising campaign, using Google Chrome extensions, affects approximately 1,7 million users. → Google Sites are used for delivering drive-by downloads. → Content Management Systems (CMS), such as WordPress and Drupal, are an attractive target for malicious actors. → Browser vulnerabilities can be used to further launch attacks.</p>	<p>a. Update the internet browser/ plugin. b. Avoid unverified plugins in CMS apps. c. Isolate applications and create a sandbox to reduce the risk of drive-by compromise attacks. d. Harden servers and services is a proactive approach to mitigate web-based attacks. This includes controlling the version of the content scripts, as well as scanning locally hosted files and scripts for the web server or service. e. Facilitate tools such as adblockers or JavaScript blockers. f. Monitor web e-mail and filter content for detecting and preventing the delivery of malicious URLs and files/payloads.</p>
Phishing	<p>→ 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. → 88% of worldwide organisations experienced spear phishing attacks and 86% of them faced Business Email Compromise (BEC) attacks (Microsoft 365 was the most targeted service with focus on harvesting credentials). → In the last quarter of 2019, 74% of phishing sites were using HTTPS, a significant increase compared with just 32% only 2 years earlier. → Threat actors may also use legitimate sites they have hacked to host phishing content, therefore making it challenging for the end-user to identify a site as unsafe. → Phishing-as-a-Service (PhaaS) is on the rise (that is a kit that helps in cloning a random website).</p>	<p>a. Educate staff to identify fake and malicious emails. b. Launch simulated phishing campaigns for testing. c. Consider the use of a security email gateway with regular maintenance of filters (anti-spam, anti-malware, policy-based filtering). d. Consider applying security solutions that use ML to identify phishing sites in real-time. e. Disable automatic execution of code, macros, rendering of graphics and preloading mailed links at the mail clients and update them frequently. f. Implement one of the standards for reducing spam e-mails: SPF, DMARC, and DKIM. g. Ideally, use secure e-mail communication using digital signatures or encryption. h. Implement fraud and anomaly detection at the network level for both inbound and outbound emails. i. Avoid clicking on random links.</p>
Web application attacks	<p>→ Two thirds of web application attacks include SQLi attacks. → The majority of web application attacks are limited to SQL injection and Local File inclusion (LFI).</p>	<p>a. Use input validation and isolation techniques for injection type attack and implement web application firewalls</p>

		<ul style="list-style-type: none"> b. Incorporate application security processes into the application development and maintenance life-cycle. c. Restrict access to inbound traffic for required services only and deploy traffic and bandwidth management capabilities. d. Enforce web application server hardening, patch management and testing processes. e. Perform vulnerability and risk assessments before and during the web application development. f. Conduct regular penetration testing during implementation and after deployment.
SPAM	<p>→Various campaigns in 2019 used the same botnet system to distribute spam messages (based on template emails from Google, Qatar Airways, FedEx, LinkedIn or Microsoft).</p> <p>→The Gamut botnet was the third most active spam botnet in 2019. Gamut messages are mostly related to suggestions for dating or meeting people, offers of pharmaceutical products and job opportunities.</p> <p>→A COVID-19 spamming campaign was reported to be spreading the Eeskiri-COVID.chm19, a disguised keylogger.</p>	<ul style="list-style-type: none"> a. Implement content filtering in email. b. Use multifactor authentication to access email accounts. c. Avoid money transfers to unverified bank accounts and logging into new links received in emails or SMS messages. d. Disable automatic code execution, macro enabling and preloading of graphics and mailed links. e. Implement SPF, DMARC, or DKIM. f. Use AI and machine learning for anomaly detection checks.
Denial of Service	<p>→SYN Flood is still considered to be challenging to mitigate based on its characteristics,</p> <p>→A record of SYN flood activity distributing 500 million packets per second (mpps) was observed targeting one organization and, subsequently, in April 2019, the volume increased to 580 mpps.</p> <p>→Web services dynamic discovery (WS-Discovery) is a multicast discovery protocol that was used as an amplification technique.</p> <p>→Malicious actors often carry out multiple vectors of DoS attacks at the application layer (HTTP Flood, DNS Flood etc.) and network layer (UDP/TCP reflection/amplification etc.)</p>	<ul style="list-style-type: none"> a. Understand services and critical resources and prioritize defence where these can be overloaded. b. Consider DDoS protection service or a DDoS managed service provider or publish services through content delivery networks. c. Facilitate cache servers or drop inappropriate queries/requests in the application layer at source and implement ingress filtering.
Identity Theft	<p>→Brands - such as Microsoft (44%) and Amazon (17%) - continue to lead in the rankings of 2019 brand impersonation attacks, however, new additions, such as the United States Internal Revenue Service (IRS), are notable.</p>	<ul style="list-style-type: none"> a. Do not use the password manager provided by the browser (use an offline protected password manager, instead). b. Authenticate any sender of a request to transfer money by telephone or in person c. Do not share sensitive information such as patient records in handwritten notes to

	<p>→A number of victims of SIM-swapping were recorded, such as Jack Dorsey (Twitter’s CEO), Jessica Alba (actor), Shane Dawson (actor), Amanda Cerny (actor, twice a victim), Matthew Smith (actor, four times victim) and King Bach (artist).</p> <p>→Attackers impersonate friends/colleagues and persuade victims to buy and send them back a gift card. The average amount stolen per gift card reached US \$1500</p>	<p>prevent their loss or misplacement; digital files are better for data with a short lifetime and then they should be completely destroyed.</p> <p>d. Use policies such as velocity-based rules to mitigate identity fraud, especially for payment card transactions.</p> <p>e. Use a single-sign-on (SSO) authentication method, when available,</p> <p>f. Install end-point protection by means of antivirus programs, but also block execution of files appropriately (e.g. block execution in the temp folder).</p> <p>g. Use multifactor authentication when possible.</p> <p>h. Check URLs that are sent by email or randomly visited.</p> <p>i. Use TLS.</p> <p>j. Enforce the use of password-protected devices.</p> <p>k. Pay close attention when using public Wi-Fi networks.</p> <p>l. Check transactions documented by bank statements or received receipts regularly for irregularities.</p> <p>m. Install content filtering to filter out unwanted attachments, emails with malicious content, spam and unwanted network traffic.</p> <p>n. Enforce data loss prevention (DLP) solutions.</p>
<p>Data breach</p>	<p>The data breach incidents increased in 2019 and 2020.</p> <p>The financial impact of a breach can remain 2 years after the incident.</p> <p>Financial gain has been identified as the main motivation behind data breaches.</p> <p>Healthcare was one of the most attractive targets for cybercriminals using ransomware and phishing techniques.</p> <p>In 2019 400 healthcare organizations reported data breaches in patient records.</p>	<p>a. Invest in hybrid data security tools that focus on operating in a shared responsibility mode for cloud-based environments.</p> <p>b. Provide training and simulation scenarios for identifying social engineering/phishing campaigns for employees.</p> <p>c. Identify and classify sensitive/personal data and apply measures for encrypting such data in transit.</p> <p>d. Increase investment in detection and alerting tools.</p> <p>e. Develop and maintain strong policies, enforcing strong passwords and use multifactor authentication.</p>
<p>Insider threat</p>	<p>There are 5 types of insider threats:</p> <p>a. Careless workers who mishandle data, break policies and install unauthorized apps</p> <p>b. Inside agents that steal information on behalf of outsiders</p> <p>c. Angry workers who want to harm their organization</p>	<p>a. Draw up a security policy on insider threat based on user awareness.</p> <p>b. Introduce an insider threat countermeasures plan into the overall security strategy and policies.</p> <p>c. Implement robust technical controls that will focus on both external and internal threats.</p>

	<p>d. Malicious insiders who use existing privilege to steal information for personal gain</p> <p>e. Careless third-parties who compromise security through intelligence</p> <p>The insider threat could execute all kill chain stages, because he has legitimate access and privileges to the system. → Cost of insider threats increased by 31% during 2019.</p>	<p>d. Reduce the number of users with privileges and access to sensitive information.</p>
<p>Botnet</p>	<p>A botnet is a network of connected devices infected by bot malware. They are typically used to conduct DDoS attacks.</p> <p>They are remotely controlled by a malicious actor through a Command and Control server. → 60% of new rival botnet activity is associated with stealing credentials</p> <p>During the first half of 2019, botnet activity and hosting Command and Control servers increased.</p> <p>Linux based botnets were responsible for almost 97.4% of attacks.</p> <p>LokiBot remained at the top of the list of credential stealing bots in 2019 → 17,602 botnet C2 servers were live during 2019, representing a 71.5% increase compared with 2018.</p>	<p>a. Understand and categorise vulnerabilities and implement a strong patching and updating practice.</p> <p>b. Restrict or block cryptocurrency mining pools.</p> <p>c. Deploy challenge-based capabilities for required websites to check the origin of traffic.</p> <p>d. Deploy and configure network and application firewalls.</p>
<p>Physical manipulation, damage, theft and loss</p>	<p>Intelligent buildings, mobile devices and smart wearables can be exploited to bypass physical security measures. New security practices for physical security:</p> <ul style="list-style-type: none"> • Proactive security policies • AI and deep learning IP camera systems • Cloud solutions • Multifactor authentication with biometrics • IoT intelligent sensors <p>Physical access is the biggest backdoor. → 54% of data breaches across all sectors included a physical attack as the main method.</p>	<p>a. Use encryption in all information storage and flow that is outside the security perimeter.</p> <p>b. Ensure limited access to areas containing sensitive information or devices.</p> <p>c. Integrate physical security measures with digital ones to have a holistic approach.</p> <p>d. Use insurance policies to cover possible losses and damages.</p> <p>e. Ensure that devices are disposed of after personal or sensitive information has been securely deleted.</p> <p>f. Implement multifactor authentication with biometrics and user credentials/physical tokens.</p> <p>g. Inspect devices periodically for alterations.</p> <p>h. Assign proper and limited access rights to each employee.</p> <p>i. Implement access monitoring systems, access control systems, strong access credentials, and smart access devices (e.g. smart locks, smart keys) for areas housing sensitive equipment.</p>

		<p>j. Most preferable alternatives for multifactor authentication: fingerprint, secure ID, sms/smartphone, facial recognition.</p>
<p>Information leakage</p>	<p>A data breach frequently causes information leakage. Information leakage is one of the major cyber threats, and is related to compromised information (PII, financial data, personal health information). There were 2013 confirmed data disclosures in 2019 (11% increase in the first half of 2019). → 14% of all incidents in the financial sector were data disclosure → 4,1 billion data records were exposed globally in the first half of 2019 Most of the incidents in 2019 were attributable to unsecured/unencrypted databases. The primary attack vector in information leakage is insiders → a person who is interested in exfiltrating important inside information on behalf of a third party.</p>	<p>a. Anonymize, pseudonymize, minimize, and cipher data in accordance with the regulation commitments for counterpart entities who do not fall under bi-lateral or multi-lateral initiatives. b. Store data only in secure IT assets. c. Limit user access privileges. d. Educate and train the personnel periodically e. Deploy data and portable system and device encryption, and secure gateways. f. A business continuity plan (BCP) is crucial for dealing with a data breach. This plan outlines the type of data being stored and their location, and what potential liabilities could arise when implementing data security and recovery actions. A BCP entails an effective incident response, which aims to address, manage and rectify the damages caused by such an incident.</p>
<p>Ransomware</p>	<p>There is a lack of legislation in the majority of countries that clearly criminalizes ransomware attacks. → 10.1 million euros estimated to be paid in ransoms during 2019 → 365% increase in ransomware machine detection in businesses in 2019 compared to 2018. → 66% of healthcare organizations experienced an attack. Most ransomware attacks exploit software vulnerabilities to enter the victim's system, install malware and encrypt the victim's files. In some cases, it also deletes the files after a specific time limit if the ransom is not paid. The most wanted: LOCKERGOGA, KATYUSHA, JIGSAW, PEWCRIPT, RYUK, DHARMA, GANDCRAB, SODINOKIBI, SAMSAM.</p>	<p>a. Maintain reliable backups that are up to date and follow the 3-2-1 rule (maintain at least 3 copies, in 2 different formats, keeping one of those copies off-site). b. Invest in a cyber insurance policy that covers ransomware damages. c. Use network segmentation, data encryption, access control and policy enforcement to ensure minimum exposure of data. d. Use appropriate and updated tools for ransomware prevention. e. Define a minimum set of access rights to users to minimize the impact of the attacks. f. Implement robust vulnerability and patch management. g. Use whitelisting to prevent executables for being executed at endpoints. h. Invest in raising users' awareness of ransomware.</p>
<p>Cyberespionage</p>	<p>Cyber espionage is considered both as a threat and a motive in cybersecurity. It is defined as "the use of computer networks to gain illicit access to confidential information, typically that held by a government or other organisation."</p>	<p>a. Assess vulnerabilities and patch the software regularly. b. Identify mission critical roles in the organization and estimate their exposure to espionage risk. c. Create whitelist for critical application services.</p>

	<p>It focuses on driving geopolitics and on stealing state and trade secrets, intellectual property rights and proprietary information.</p> <p>In 2019, the number of nation-state-sponsored cyberattacks targeting the economy rose.</p> <p>→ 38% of malicious actors are connected with nation states.</p> <p>→ 11.2% of incidents are motivated by cyber espionage</p> <p>→ 63% of cyber espionage incidents involved phishing</p>	<p>d. Establish content filtering on all inbound and outbound channels.</p>
<p>Cryptojacking</p>	<p>It is the unauthorized use of a device's resources to mine cryptocurrencies. Cybercriminals have been increasingly targeting cloud infrastructures. This type of attack has not attracted much attention from law enforcement agencies, mainly because of its relatively few negative consequences.</p> <p>How to detect crypto mining: higher IT costs, degraded computer components, increased electricity consumption, reduced employee productivity caused by slower work stations</p> <p>→ 64.1 million cryptojacking hits by the end of 2019</p> <p>→ 78% decrease in cryptojacking activities in the second half of 2019 compared with the first half.</p> <p>The first most active miner is trojan Win32.Miner.bbb (13%).</p> <p>In 2019, there was a downwards trend in cryptojacking attacks, mainly due to the closure of Coinhive, the coordinated efforts of law enforcement agencies, and the depreciation of the Monero cryptocurrency.</p>	<p>a. Monitor battery usage.</p> <p>b. Implement content filtering to filter out unwanted attachments, emails with malicious content and spam.</p> <p>c. Blacklist the IP addresses and domains of known mining pools.</p> <p>d. Install antivirus programs or crypto miner blocking browser plugins.</p> <p>e. Conduct regular security audits to detect network anomalies.</p> <p>f. Use whitelisting to prevent unknown executables from being executed at endpoints.</p>

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 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 document, the second roadmap in the series, focused on

1. *updating the research priorities*, introducing any new research topics, and possibly readjusting the ranking of existing ones
2. providing a *SWOT analysis* that builds on strengths and addresses shortcomings:
 - what are the strengths of Europe in these verticals?
 - what are the weaknesses?
 - what (global) opportunities may exist?
 - what threats should we be careful of?
3. explaining how the chosen research priorities interact with the *important dimensions* of European policies in 2020-2021 as they relate to:
 - the **European Digital Sovereignty**,
 - the new reality imposed by **COVID-19**, and
 - the **Green Deal**.

Partially based on the above dimensions, and using a uniform methodology, each vertical produced a roadmap in three phases: short term (for the next 12 months), medium term (for next two years), and long term which includes challenges to be addressed after the end of this project.

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. Available online: ftp://ftp-boi.external.hp.com/pub/catia/HP_PWS/MS_KB/xpsp2.doc (accessed: November 2020).
- [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. <https://www.rolls-royce.com/media/press-releases/2016/pr-12-04-2016-aawa-project-introduces-projects-first-commercial-operators.aspx> [Accessed 29 November 2020]
- [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* (2020): 104941.
- [ABEL 2009] Abadi, Martín, Mihai Budiu, Úlfar Erlingsson, and Jay Ligatti. “Control-flow integrity principles, implementations, and applications.” *ACM Transactions on Information and System Security (TISSEC)* 13, no. 1 (2009): 1-40.
- [Abulamddi 2017] Abulamddi, Mohammedab FH. “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.
- [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.
- [AKLT 2020] Amro, Ahmed, Georgios Kavallieratos, Konstantinos Louzis and Cristoph A. Thieme. “Impact of cyber risk on the safety of the MilliAmpere2 Autonomous Passenger Ship.”. In Proceedings of the 3rd International Conference on Maritime Autonomous Surface Ship (ICMASS 2020), 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). Online available: <https://www.ssi.gouv.fr/guide/ebios-risk-manager-the-method/> (accessed: November, 2020).

[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.

[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.

[AUTOSHIP 2019]. EU H2020 project "Autonomous Shipping Initiative for European Waters", 2019. Available online: <https://www.autoship-project.eu/> (accessed: November 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.

[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.

[BBC+ 2019] Baldini, G., Barrero, J., Chaudron, S., Coisel, I., Draper Gil, G., Duch Brown, N., Eulaerts, O., Geneiatakis, D., Hernandez Ramos, J., Joanny, G., Junklewitz, H., Kampourakis, G., Kerckhof, S., Kounelis, I., Lewis, A., Martin, T., Nai Fovino, I., Nativi, S., Neisse, R., Nordvik, J., Papameletiou, D., Reina, V., Ruzzante, G., Sanchez Martin, J., Sportiello, L., Steri, G. and Tirendi, S., Cybersecurity, our digital anchor, Nai Fovino, I., Barry, G., Chaudron, S., Coisel, I., Dewar, M., Junklewitz, H., Kampourakis, G., Kounelis, I., Mortara, B., Nordvik, J. and Sanchez Martin, J. editor(s), EUR 30276 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-19957-1 (online),978-92-76-19958-8 (print), doi:10.2760/352218 (online),10.2760/967437 (print), JRC121051.

[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.

[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.

[BDF+ 2020] Baumgärtner, Lars, Alexandra Dmitrienko, Bernd Freisleben, Alexander Gruler, Jonas Höchst, Joshua Kühlberg, Mira Mezini et al. "Mind the GAP: Security & Privacy Risks of Contact Tracing Apps." arXiv preprint arXiv:2006.05914 (2020).

[BDL+ 2019] Bartolini, Cesare, Said Daoudagh, Gabriele Lenzini, and Eda Marchetti. "Towards a Lawful Authorized Access: A Preliminary GDPR-based Authorized Access." ICISOFT 2019 (2019): 331-338.

[BDVA] López de Vallejo, I., Scerri, S., Tuikka, T. (eds) (2020) Towards a European-Governed Data Sharing Space. Brussels. https://www.bdva.eu/sites/default/files/BDVA%20DataSharingSpaces%20PositionPaper%20V2_2020_Final.pdf (accessed: November 2020)

[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.

[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.

[BEF19] 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] Bécue, 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.

[BGL+ 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.

[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] Bernal Bernabe, Jorge, Jose L. Hernandez-Ramos, and Antonio F. Skarmeta Gomez. "Holistic privacy-preserving identity management system for the internet of things." *Mobile Information Systems* 2017 (2017).

[BIMCO 2018] Baltic and International Maritime Council. (BIMCO), "The guidelines on cyber security onboard ships". Version 3.0., 2018.

[BIZJAK 2019] T. BIZJAK, "Sacramento, Calif., Transit System Recovers from Ransomware Attack," 22 November 2017. <https://www.govtech.com/security/Sacramento-Calif-Transit-System-Recovers-from-Ransomware-Attack.html> (accessed: December 2019).

[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] Bellare, Steven Michael, and Michael Merritt. "Encrypted key exchange: Password-based protocols secure against dictionary attacks." In *Proceedings of the 1992 IEEE Computer Society Symposium on Research in Security and Privacy*, pages 72–84. IEEE, 1992.

[BN 2014] Backes, Michael, and Stefan Nürnberg. "Oxymoron: making fine-grained memory randomization practical by allowing code sharing." In *Proceedings of the 23rd USENIX conference on Security Symposium*, pp. 433-447. 2014.

[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.

[Brewster 2016] T. Brewster, "Ransomware Crooks Demand \$70,000 After Hacking San Francisco Transport System," <https://www.forbes.com/sites/thomasbrewster/2016/11/28/san-francisco-muni-hacked-ransomware/> (accessed: December 2019).

[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.

[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).

[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.

[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).

[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). Online available: <http://meharipedia.x10host.com/wp/telechargements/document2/> (accessed: December 2020).

[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] Calabró, 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 1982] 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.

[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, <https://clang.llvm.org/docs/ControlFlowIntegrity.html> (accessed: November 2020)

[CMB+ 2011] Cimpan, Dan, Johan Meire, Vincent Bouckaert, Stijn Vande Castele, Aurore Pelle, and Luc Hellebooge. “Analysis of cyber security aspects in the maritime sector.” (2011), https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1/at_download/fullReport (accessed: December 2020)

[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] French Commission Nationale de l’Informatique et des Libertés. The open source PIA software helps to carry out data protection impact assessment. Retrieved from <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment>

[COMPACT 2018] COMPACT Project, “Overall COMPACT architecture,” (H2020 Project, G.A.740712), 2018. <https://www.compact-project.eu/deliverables/D3.2%20Overall%20COMPACT%20architecture.pdf> (accessed: December 2020)

[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).

[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.; Rodney J. Simmons (March 1998). System Safety and Risk Management. NIOSH Instructional Module, A guide for Engineering Educators. Cincinnati, OH: National Institute for Occupational Safety and Health: IX-3–IX-7.

[CS 2017] Cui, Jin, and Giedre Sabaliauskaite. “On the alignment of safety and security for autonomous vehicles.” IARIA Cyber (2017).

[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.

[CSS, 1999] Custer, R. L., Scarcella, J. A., & Stewart, B. R. (1999). JVTE v15n2: The modified Delphi technique-A rotational modification. Journal of Vocational and Technical Education, 15(2), Spring 1999. Online available: <https://scholar.lib.vt.edu/ejournals/JVTE/v15n2/custer.html> (accessed: November 2020).

[CYBER 2005] President's Information Technology Advisory Committee. Cyber security: A crisis of prioritization. National Coordination Office for Information Technology Research and Development, 2005.

[CySiMS] Cyber Security in Merchant Shipping. <http://cysims.no/>

[Daffey 2018] Daffey, K., “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. Online available: https://wwwcdn.imo.org/localresources/en/MediaCentre/IMOMediaAccreditation/Documents/MSC%20100%20special%20session%20presentations/20181203_Technology_Progression_In_MASS_IMO_Final_For_PDF.pdf (accessed: November 2020).

[DBL 2019] De Benedictis, Marco, and Antonio Lioy. “A proposal for trust monitoring in a Network Functions Virtualisation Infrastructure.” In 2019 IEEE Conference on Network Softwarization (NetSoft), pp. 1-9. IEEE, 2019.

[DECLERCQ 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.” Aja, The Atlanta Journal-Constitution 2 (2018).

[Deloitte 2019] Deloitte Insights, “Making smart cities cybersecure,” 2019.

[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." Available at SSRN 3606261 (2020).

[DSL018] 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.

[DVN GL 2020] DNV GL. Digitalization in the maritime industry. <https://www.dnvgl.com/maritime/insights/topics/digitalization-in-the-maritime-industry/index.html> (accessed: November 2020)

[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 (SIN), pp. 77–84, ACM, 2014.

[EBS] Edinburh Business School. Privacy by Design and Data Protection Impact Assessment (DPIA) Toolkit. Retrieved from <https://www.hw.ac.uk/documents/privacy-by-design-dpia-toolkit.pdf>

[EC 2018] European Commission. "Maritime: What do we want to achieve?" Mobility and Transport. https://ec.europa.eu/transport/modes/maritime_en (accessed December 2020)

[EC 2019] European Commission report 2016-2019, Maritime Affairs and Fisheries, What is the Blue Economy? https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/publications/what-is-the-blue-economy_en_1.pdf (accessed: November 2020).

[EC725/2004] EUROPEAN PARLIAMENT AND COUNCIL. IN: Official Journal of the European Union 2004

[ECS+ 2015] Everspaugh, Adam, Rahul Chatterjee, Samuel Scott, Ari Juels, and Thomas Ristenpart. "The pythia PRF service." In Proceedings of the 24th USENIX Conference on Security Symposium, 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," 22 March 2010. https://ec.europa.eu/commission/presscorner/detail/en/EDPS_10_6 (accessed: December 2019).

[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] Khaled El Emam, PhD, Fida Kamal Dankar, MSc, "Protecting Privacy Using k-Anonymity", Journal of the American Medical Informatics Association, Volume 15, Issue 5, September 2008, Pages 627–637, <https://doi.org/10.1197/jamia.M2716>

[EMSA 2020A] European Maritime Safety Agency (EMSA), SafeSeaNet main page,
<http://www.emsa.europa.eu/ssn-main.html>

[EMSA 2020B] EMSA November 11th Report, COVID-19 – Impact on shipping

[ENISA 2011] ENISA, EU. Cimpean, D., Meire, J., Bouckaert, V., Vande Casteele, S., Pelle, A., & Hellebooge, L., “Analysis of cyber security aspects in the maritime sector”, November 2011.

[ENISA 2014] ENISA, “Secure ICT Procurement in Electronic Communications,” 2014,
<https://www.enisa.europa.eu/publications/secure-ict-procurement-in-electronic-communications/>
(accessed: December 2020)

[ENISA 2015] ENISA, “Supply Chain Integrity: An overview of the ICT supply chain risks and challenges, and vision for the way forward,” 2015, <https://www.enisa.europa.eu/publications/sci-2015> (accessed: December 2020)

[ENISA 2017] ENISA, “Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures,” 2017, <https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot> (accessed: December 2020)

[ENISA 2017A] ENISA, “Communication network dependencies for ICS/SCADA Systems,” 2017,
<https://www.enisa.europa.eu/publications/ics-scada-dependencies> (accessed: December 2020)

[ENISA 2018] ENISA, “Good Practices for Security of Internet of Things, in the context of Smart Manufacturing,” 2018, <https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot>
(accessed: December 2020)

[ENISA 2019] ENISA, “Port cybersecurity-good practices for cybersecurity in the maritime sector,” 2019,
<https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector> (accessed: December 2020)

[ENISA 2019A] ENISA, Industry 4.0 Cybersecurity: Challenges & Recommendations, 2019,
<https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations>
(accessed: December 2019).

[ENISA 2020] ENISA, “Inventory of Risk Management / Risk Assessment Method”
<https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods> (accessed: October 2020).

[ENISA 2020B] ENISA, “ENISA Threat Landscape – 2020,” <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends> (accessed: December 2020).

[ENISA 2020C] ENISA, “Guidelines for Securing the Internet of Things,”
<https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things> (accessed: December 2020)

[ENISA 2020D] ENISA, “Standardisation in support of the Cybersecurity Certification,”
<https://www.enisa.europa.eu/publications/recommendations-for-european-standardisation-in-relation-to-csa-i> (accessed: December 2020)

[ENISA 2020E] ENISA, EU. Drougkas A., Sarri A., Kyranoudi P. “Cyber Risk Management for Ports. Guidelines for cybersecurity in the maritime sector”, December, 2020.

[ENISA 2020F] ENISA, “AI Cybersecurity Challenges,” 2020, <https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges> (accessed: January 2021)

[EPCCert 2010] EPCGlobal, EPCGlobal Certificate Profile Specification, June 2010, https://www.gs1.org/sites/default/files/docs/cert/cert_2_0-standard-20100610.pdf (accessed: December 2021)

[EPRS 2020] European Parliamentary Research Service, Tambiama Madiega, “Digital sovereignty for Europe”, PE 651.992, July 2020.

[Ercan 2007] Mehmet Ercan Nergiz, Maurizio Atzori, Cris Clifton. “Hiding the presence of individuals from shared databases” [SIGMOD '07: Proceedings of the 2007 ACM SIGMOD international conference on Management of data](#) June 2007 Pages 665–676 <https://doi.org/10.1145/1247480.1247554>

[Ericson, 1999] Ericson, C. (1999). Fault Tree Analysis - A History. Proceedings of the 17th International Systems Safety Conference. Archived from the original on 2011-07-23. Online available: <https://web.archive.org/web/20110723124816/http://www.fault-tree.net/papers/ericson-fta-history.pdf> (accessed: November 2020)

[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). Available online: <https://eur-lex.europa.eu/eli/reg/2019/881/oj> (accessed: November 2020)

[EU 2020] European Union. Blue Growth. https://ec.europa.eu/maritimeaffairs/policy/blue_growth_en (accessed: November 2020).

[Europol 2020] Europol, “Internet Organized Threat Assessment”, <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020>, 2020 (accessed: November 2020).

[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.

[FBM 2017] Frøystad, Christian, Karin Bernsmed, and Per Håkon Meland. “Protecting Future Maritime Communication.” In Proceedings of the 12th International Conference on Availability, Reliability and Security, pp. 1-10. 2017.

[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.

[FIRST] FIRST, “Common Vulnerability Scoring System version 3.1,” https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf.

[FLN] Family Links Network. Template for Data Protection Impact Assessment (DPIA). Retrieved from 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+ et al. 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.

[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.

[Gagniuc 2017] Gagniuc, Paul A. (2017). Markov Chains: From Theory to Implementation and Experimentation. USA, NJ: John Wiley & Sons. pp. 1–235. ISBN 978-1-119-38755-8.

[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 (2020).

[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 & Decisions (2020): 1.

[GK+ 2004] Grance, Tim, Karen Kent, and Brian Kim. “Computer security incident handling guide.” NIST Special Publication 800, no. 61 (2004): 11.

[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, Nelson Humberto 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.

[Gonzalez 2005] Gonzalez, Jose J. "Towards a cyber security reporting system—a quality improvement process." In International Conference on Computer Safety, Reliability, and Security, pp. 368-380. Springer, Berlin, Heidelberg, 2005.

[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.

[Granger 2001] Granger, Sarah. "Social engineering fundamentals, part I: hacker tactics." Security Focus, December 18 (2001).

[GREENDEAL] "A European Green Deal, Striving to be the first climate-neutral continent" https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_en (accessed: November 2020)

[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 (2020).

[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.

[Gueham 2015] Gueham, Farid. "Digital Sovereignty-Steps Towards a New System of Internet Governance." Paris: Fondapol (2017).

[HACKREAD 2019] HACKREAD, "Baltimore' 911 CAD system hacked; remained suspended for 17 hours," 28 March 2018. <https://www.hackread.com/baltimore-911-cad-system-hacked-suspended/>. (accessed: December 2019).

[Hardt 2012] Hardt, Dick. The OAuth 2.0 authorization framework. RFC 6749, October, 2012.

[Hastings 1970] Hastings, W. K. (1970). "Monte Carlo sampling methods using Markov chains and their applications". Biometrika. 57(1): 97–109. DOI:10.1093/biomet/57.1.97. ISSN:0006-3444. S2CID 21204149

[HH 2011] Hammer-Lahav, D. E., & Hardt, D. (2011). The oauth2. 0 authorization protocol. 2011. <https://tools.ietf.org/html/draft-ietf-oauth-v2-22> (accessed: December 2020).

[HHKSR 2017] Höyhtyä, 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.

[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* (2020).

[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.

[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.

[Hobson, 2020] Hobson, F. (2020). “50% of enterprises and system integrators say it is impossible to comply with the GDPR without a centralised identity management solution.” <https://www.ubisecure.com/news-events/organisations-say-gdpr-compliance-impossible-without-ciam/> (accessed: November 2020)

[HOM+ 2017] Höyhtyä, 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.” <https://eprint.iacr.org/2020/657> (accessed: December 2020)

[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.

[HSMC20] David M. Higgins II, P. (2020). New research: An average person has more passwords than an average pop song has words. *The Southern Maryland Chronicle*. Retrieved from <https://southernmarylandchronicle.com/2020/02/26/new-research-an-average-person-has-more-passwords-than-an-average-pop-song-has-words/>

[IATF16949 2016] IATF, Quality Management System Requirements for Automotive Production and Relevant Service Parts Organization, October 2016, <https://www.aiag.org/quality/iatf16949> (accessed: December 2020)

[ICO] Information Commissioner's Office. Data protection impact assessments. Retrieved from <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/>

[IESE 2019] IESE Business School, "IESE Cities in Motion Index 2019," University of Navarra, 2019.

[IEP 2017] Institute for Economics & Peace (IEP) , "Global Terrorism Index 2017," 2017, <https://reliefweb.int/report/world/global-terrorism-index-2017> (accessed: December 2020)

[IHO 2015] IHO, 2015, IHO Data Protection Scheme Edition 1.2.0, January 2015, IHO Publication S-63, International Hydrographic Bureau, Monaco.

[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] Intel IT, "Threat Agent Library Helps Identify Information Security Risks," 2007.

[IMO 2003] International Maritime Organization. International Convention for the Safety of Life at Sea (SOLAS) chapter XI-2 2003

[IMO 04] International Maritime Organization. Solas, Consolidated Edition, 2004: Consolidated Text of the International Convention for the Safety of Life at Sea. Online Available: http://library.arcticportal.org/1696/1/SOLAS_consolidated_edition2004.pdf (accessed: December 2020)

[IMO 2017A] List of certificates and documents under IMO instruments required to be carried out onboard ships (arrival, stay and departure of ships). FAL.2/Circ.131, 19 July, 2017. Available online: <https://www.register-iri.com/wp-content/uploads/FAL.2-CIRC.131.pdf> (accessed: November 2020)

[IMO 2017B] Guidelines on Maritime cyber risk management. MSC-FAL.1/Circ.3, 5 July, 2017. Available online: <https://www.samgongustofa.is/media/english/MSC-FAL.1-Circ.3---Guidelines-On-Maritime-Cyber-Risk-Management--Secretariat-.pdf> (accessed: November 2020).

[IMO 2020] International Maritime Organization, 2020, MSC.1/Circ.1294/Rev.6, 8 April 2020 Long-Range Identification and Tracking System, Technical Documentation (Part I and II).

[IP Bank 2015] IP Bank B.V., CGE Risk Management Solutions B.V., The next generation BowTie methodology Tool. Rev.15, 2015. Online available: <https://www.icao.int/safety/SafetyManagement/SMI/Documents/BowTieXP%20Methodology%20Manual%20v15.pdf> (accessed: December 2020).

[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, <https://www.iso.org/standard/50341.html> (accessed: December 2020)

[ISO/IEC27000 2018] ISO, 27000:2018: Information technology – Security techniques – Information security management systems – Overview and vocabulary, 5th Edition, February 2018, <https://www.iso.org/standard/73906.html> (accessed: in October 2020)

[ISO20858 2007] ISO, 20858:2007: Ships and marine technology – Maritime port facility security assessments and security plan development, 1st Edition, October 2007, <https://www.iso.org/standard/46051.html> (accessed: in October 2020)

[ISO/IEC27001 2013] ISO, 27001:2013: Information technology – Security techniques – Information security management systems – Requirements, 2nd Edition, October 2013, <https://www.iso.org/standard/65694.html> (accessed: in October 2020)

[ISO/IEC27002 2013] ISO, 27002:2013: Information technology – Security techniques – Code of practice for information security controls, 2nd Edition, October 2013, <https://www.iso.org/standard/54533.html> (accessed: in October 2020)

[ISO/IEC27005 2018] ISO, 27005:2018: Information technology — Security techniques — Information security risk management, 3rd Edition, July 2018, <https://www.iso.org/standard/75281.html> (accessed: October 2020)

[ISO/IEC20243-1 2018] ISO, 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, <https://www.iso.org/standard/74399.html> (accessed: December 2020)

[ISO 2019] ISO, ISO 28000:2007: Specification for security management systems for the supply chain, September 2007, <https://www.iso.org/standard/44641.html> (accessed: December 2019)

[ISO31000 2018] ISO, 31000:2018: Risk Management – Guidelines, 2nd Edition, February 2018, <https://www.iso.org/standard/65694.html> (accessed: October 2020)

[ISO/IEC31010 2019] ISO, 31010:2019: Risk management — Risk assessment techniques, 2nd Edition, June 2019, <https://www.iso.org/standard/72140.html> (accessed: October 2020)

[Jensen 2020] Thomas Jensen (editor): “D3.2: Updated SPARTA SRIA (Roadmap v1)”, <https://www.sparta.eu/assets/deliverables/SPARTA-D3.2-Updated-SPARTA-SRIA-roadmap-v1-PU-M12.pdf>, 2020 (last access November 2020). Ssas”

[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).

[Johnson 2015] Johnson, Chris W. "Architectures for cyber-security incident reporting in safety-critical systems." In *Disaster Management: Enabling Resilience*, pp. 127-141. Springer, Cham, 2015.

[JRC 2019] Nai Fovino, I., Neisse, R., Hernandez Ramos, J., Polemi, N., Ruzzante, G., Figwer, M. and Lazari, A., A Proposal for a European Cybersecurity Taxonomy, EUR 29868 EN, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-11603-5 (online), doi:10.2760/106002 (online), JRC118089.

[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.

[KA 2019] L. Kearney and L. Adler, "Atlanta officials reveal worsening effects of cyber attack," 7 June 2018. <https://www.reuters.com/article/us-usa-cyber-atlanta-budget/atlanta-officials-reveal-worsening-effects-of-cyber-attack-idUSKCN1J231M> (accessed: December 2019).

[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 Katsikas. "Shipping 4.0: Security requirements for the Cyber-Enabled Ship." *IEEE Transactions on Industrial Informatics* (2020).

[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.

[Kežmah 2020] CyberSec4Europe Deliverable D3.6 Guidelines for GDPR Compliant User Experience. CyberSecurity4Europe project. Editor Boštjan Kežmah 2020.

[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] G. Kavallieratos, S. Katsikas, and V. Gkioulos. Cybersecurity and safety co-engineering of cyberphysical systems - a comprehensive survey. *Future Internet*, 12(4):65, 2020.

- [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.
- [KLNT2011] D. Kokotos, D. Linardatos, N. B. Nikitakos, and E. S. Tzannatos. Information and communication technologies in shipping industry (In Greek), 2011.
- [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.
- [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, S., Lorünser, T., Salzer, A. and Striecks, C., 2017, November. Towards attribute-based credentials in the cloud. In International Conference on Cryptology and Network Security (pp. 179-202). Springer, Cham.
- [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.
- [KMS+ 2016] Kosba, Ahmed, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts." In 2016 IEEE symposium on security and privacy (SP), pp. 839-858. IEEE, 2016.
- [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] Kuznetzov, 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.
- [Loyds 2016] Lloyds Register. Cyber-enabled ships. page 20, 2016.

[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.

[Lee 2017] Lee, C. A Study on Introducing Cyber Security Incident Reporting Regulations for Nuclear Facilities, CYBER 2017, https://www.thinkmind.org/articles/cyber_2017_4_20_80046.pdf (accessed January 2021).

[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.

[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.” Advances in Information Sciences and Service Sciences 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 2011] 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-Arcentales, 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, September 2020, Is Covid-19 accelerating digital engagement in maritime? <https://www.ship-technology.com/features/is-covid-19-accelerating-digital-engagement-in-maritime/>, (accessed November 2020).

[Markatos 2020] Evangelos Markatos (editor): “Research and Development Roadmap I”, 2020, <https://cybersec4europe.eu/wp-content/uploads/2020/09/D4.3-Roadmap-v5-NEW.pdf> (last access November 2020)

[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.

[MB 2013] E. Markatos and D. Balzarotti, *The RED BOOK: A Roadmap for Systems Security Research*, 2013.

[MBG+ 2020] Moreno, Rafael Torres, Jorge Bernal Bernabe, Jesús García Rodríguez, 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.

[MCP 2020] MCP consortium, 2020, Maritime Connectivity Platform (MCP), <https://maritimeconnectivity.net/> (accessed: November 2020)

[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.

[MG 2018] 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.

[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*, 2009.

[Min 2019] Min, Hokey. “Blockchain technology for enhancing supply chain resilience.” *Business Horizons* 62, no. 1 (2019): 35-45.

[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): 69-75.

[MSW 2006] Mitnick, Kevin D., William L. Simon, and S. Wozniak. “The Art of Deception: Controlling the Human Element of Security. 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, <http://www.unmanned-ship.org/munin/> (accessed: December 2020).

[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).

[NIST 2012] “NIST Special Publication 800-30 R1: Guide for Conducting Risk Assessments,” NIST, Gaithersburg, MD, United States., 2012

[NIST 2015] NIST, *Supply Chain Risk Management. Practices for Federal Information Systems and Organizations*, NIST SP 800-161, April 2015.

- [NIST 2015] NIST, Guide to Industrial Control Systems (ICS) Security, NIST SP 800-82, May 2015.
- [NIST 2018] NIST, Framework for Improving Critical Infrastructure Cybersecurity, v1.1, April 2018, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> (accessed: December 2019).
- [NIST 2018b] NIST, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, NIST SP 800-37, Rev.2, December 2018.
- [NIST 2019] NIST, Cyber Supply Chain Risk Management, 2019 <https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management> (accessed: December 2019).
- [NIST 2020] NIST, Performance Measurement Guide for Information Security, NIST SP 800-55, Rev.1, July 2020.
- [NIST 2020b] NIST, Case Studies in Cyber Supply Chain Risk Management (Observations from Industry) – Summary of Findings and Recommendations, 2020 <https://doi.org/10.6028/NIST.CSWP.02042020-1> (accessed: December 2020)
- [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.
- [NR 2017] H. Nordahl Ø. J. Rødseth. Nfas-definitions for autonomous merchant ships. 10 2017. Norwegian Forum for Autonomous Ships (NFAS). <https://nfas.autonomous-ship.org/wp-content/uploads/2020/09/autonom-defs.pdf> (accessed: November 2020)
- [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 Laverty, 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.

[PaX 2003] PaX TEAM, “Address space layout randomization (ASLR),” 2003. <https://pax.grsecurity.net/docs/aslr.txt> (accessed: December 2020).

[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. IEEE, 2018.

[PJB+ et al, 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, A., Kalloniatis, C. and Gritzalis, S., 2017. Security and privacy requirements engineering methods for traditional and cloud-based systems: A review. CLOUD COMPUTING 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.

[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.

[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.

[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*. No. INL/CON-05-00093. Idaho National Laboratory (INL), 2005.

[PRG+ 2020] Pérez, S., Hernández-Ramos, J.L., Matheu-García, S.N., Rotondi, D., Skarmeta, A.F., Straniero, L. and Pedone, D., 2018. A lightweight and flexible encryption scheme to protect sensitive data in smart building scenarios. *IEEE Access*, 6, pp.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.

[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.

[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 (2017).

[PWC 2020] PriceWaterhouseCoopers, 2020, *Cyber Security in Shipping during COVID-19 pandemic*, online available <https://www.pwc.com/gr/en/industries/cybersecurity-in-shipping-industry.html> (accessed December 2020)

[PZ 2013] C. Paquin, G. Zaverucha: *U-prove cryptographic specification v1.1 (revision 2)*. Tech. rep., Microsoft Corporation, April 2013

[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.

[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).

[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.

[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. Available online at: <https://iumi.com/news/news/bimco-the-guidelines-on-cyber-security-onboard-ships> (accessed: January 2021).

[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).

[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 Kobo Techno-Oceans (OTO), pp. 1-7. IEEE, 2018.

[RLG 2018] Román-Castro, Rodrigo, Javier López, and Stefanos Gritzalis. "Evolution and trends in iot security." Computer 51, no. 7 (2018): 16-25.

[RP 2018] Ribeiro, Joao 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. <https://www.rolls-royce.com/~media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/aawa-whitepaper-210616.pdf> (accessed: December 2020).

[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 Siswantoro. "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.
- [SafetyatSea 2020] Cousins S. Increased cyber-attacks during COVID-19 highlights maritime industry vulnerabilities. SafetyatSea, September 2020. Available online: <https://safetyatsea.net/news/2020/increased-cyber-attacks-during-covid-19-highlights-maritime-industry-vulnerabilities/> (accessed: November 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 IACR International Conference on Public-Key Cryptography, pp. 628-656. Springer, Cham, 2020.
- [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] Security System for Maritime Infrastructures, Ports and Coastal zones (SECTRONIC) project. European Commission. CORDIS. Online available: <https://cordis.europa.eu/project/id/218245/reporting> (accessed: November 2020)
- [Sforzin 2020] CyberSec4Europe Deliverable D3.11 Definition of Privacy by Design and Privacy Preserving Enablers CyberSecurity 4 Europe project. Editor Alessandro Sforzin 2020.
- [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.
- [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).

[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.

[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.

[Sonatype 2020] Sonatype (2020). 2020 State of the Software Supply Chain https://www.sonatype.com/hubfs/Corporate/Software%20Supply%20Chain/2020/SON_SSSC-Report-2020_final_aug11.pdf. Accessed: December 2020.

[SSN+ 2020] Saad, Muhammad, Jeffrey Spaulding, Laurent Njilla, Charles Kamhoua, Sachin Shetty, Dae Hun Nyang, and David Mohaisen. "Exploring the Attack Surface of Blockchain: A Comprehensive Survey." *IEEE Communications Surveys & Tutorials* (2020).

[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.

[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.

[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 (2020): 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." (2020). Online available: <https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=644636> (accessed: December 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, *Maritime Security: Elements of Analytical Framework for Compliance Measurement and Risk Assessment*, 2006. https://unctad.org/system/files/official-document/sdtetlb20054_en.pdf (accessed: December 2020).

[UNCTAD 2020] UNCTAD, *Review report of Maritime Transport*, United Nations Publications, 2020. <https://unctad.org/webflyer/review-maritime-transport-2020> (accessed: December 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.

[vdVGC+ 2016] Victor van der Veen, Enes Göktaş, Moritz Contag, Andre Pawloski, Xi Chen, Sanjay Rawat, Herbert Bos, Thorsten Holz, Elias Athanasopoulos, and Cristiano Giuffrida. In *Proceedings of the 37th Symposium on Security and Privacy (Oakland)*. San Jose, CA, US, May 2016.

[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.

[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.

[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* (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.

[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.

[ZPM+ 2014] Zavattoni, Eric, Luis J. Dominguez Perez, Shigeo Mitsunari, Ana H. Sánchez-Ramírez, Tadanori Teruya, and Francisco Rodríguez-Henríquez. "Software implementation of an attribute-based encryption scheme." *IEEE Transactions on Computers* 64, no. 5 (2014): 1429-1441.

[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.