Proposal No. 830929
Call H2020-SU-ICT-03-2018

Project start: February 1, 2019
Project duration: 42 months

Cyber Security for Europe

D4.3

Research and Development Roadmap 1

Document Identification	
Due date	31st January 2020
Submission date	31st January 2020
Revision	5.0 14th September 2020

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

Abstract:
This is the first 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.

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.

Executive Summary

This document presents a CyberSecurity Roadmap for the seven verticals identified in the CyberSec4Europe project: (i) Open Banking, (ii) Supply Chain, (iii) Privacy-preserving Identity Management, (iv) Security Incident Reporting, (v) Maritime Cybersecurity, (vi) Medical Data Exchange, and (vii) Smart Cities.
To be able to present their research challenges in a uniform way, all verticals followed a common structure (to the extent possible) as shown below:

- *Introduction*
  - ***Big Picture**: What is the broad setting of the vertical?*
  - *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?*
- *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**?*

The above structure helped the verticals present their challenges in a uniform way that can be understood by a person not directly involved.

The first step in identifying the research challenges in a vertical is understanding who the attackers are. We observed that the most typical attackers include hackers, (economic/market) competitors, insiders, mobsters[1], activists, governments, irrational people and even terrorists. Even further, hackers, competitors, and insiders top the list of attackers in all cases.

Once the attackers are known, the next step is to understand what kind of research needs to be done in order to defend against them. Although different verticals identified different research challenges, we see that (i) Data Security and Privacy, (ii) Legal aspects, (iii) Security Management and Governance, and (iv) Network and Distributed Systems are challenges that are usually found at the top the list for most verticals.

The remainder of this document is organized as follows: Section 2 introduces the document and section 3 describes the methodology we used to collect the needed information. Sections 4 to 10 describe the roadmap for each and every one of the verticals of the project. Section 11 presents the research challenges in the light of the JRC Taxonomy on cybersecurity and section 12 summarizes the document. Finally, Annex I presents the detailed methodology and Annex II presents related work.

[1] Individuals high in the command chain of organized crime who have significant resources available.

Document information

Contributors

Name	Partner
Cristina Alcaraz	UMA
Ahmad Amro	NTNU
Marco Angelini	Engineering
Elias Athanasopoulos	UCY
Jorge Bernal	UMU
Karin Bernsmed	SINTEF
Panagiotis Bountakas	UPRC
Laura Chinellato	BBVA
Laura Colombini	ISGS
Jérémy Decis	Dawex
Christos Douligeris	UPRC
Vasileios Gkioulos	NTNU
David Goodman	TDL
Christos Grigoriadis	UPRC
Alba Hita	UMU
Marko Hölbl	UM
Wouter Joosen	KUL
Elma Kalogeraki	UPRC
Georgios Kavalieratos	NTNU
Marko Kompara	UM
Panagiotis Kotzanikolaou	UPRC
Antonio Lioy	POLITO
Evangelos Markatos	FORTH
Per Håkon Meland	SINTEF
Vincenzo Napolitano	Engineering
Aida Omerovic	SINTEF
Spyros Papastergiou	UPRC
Ivan Pashchenko	UNITN
Juan Carlos Pérez Baún	Atos
Rodrigo Roman	UMA
Vincenzo Savarino	Engineering
Antonio Skarmeta	UMU
Krenn Stephan	AIT
Rafael Torres	UMU
Christos Xenakis	UPRC
Susana González Zarzosa	ATOS

Reviewers

Name	Partner
Elias Athanasopoulos	UCY
Javier Lopez	UMA
Kai Rannenberg	GUF
Ahad Niknia	GUF

History

Version	Date	Authors	Comment
0.01	November 1st 2019	Evangelos Markatos	Table of Contents
1.0	December 24th 2019	Evangelos Markatos (and all co-authors)	First draft for review
1.1	January 2nd 2020	Kai Rannenberg	First High-level Review
1.2	January 22nd 2020	Evangelos Markatos (and all co-authors)	Final version for High-level Review
1.2	January 24th 2020	Ahad Niknia	High-level Review
2.0	January 28th 2020	Evangelos Markatos	Final version for submission
3.0	June 30th 2020	Evangelos Markatos	Updated version
4.0	July 31st 2020	Evangelos Markatos	Address the comments of the reviewers
4.1	August 12th 2020	Ahad Niknia	High level Review
5.0	August 17th	Evangelos Markatos	Addressed comments of High-level Review

Table of Contents

List of Figures

List of Tables

List of Acronyms

A	**ABC**	Attribute-Based Credentials
	AISP	Account Information Service Provider
	API	Application Program Interface
	ASPSP	Account Servicing Payment Service Provider
C	**CERT**	Cyber Emergency Response Team
	CII	Critical Information Infrastructure
	CPS	Cyber Physical Systems
	CS4E	CyberSec4Europe
D	**DEP**	Data Exchange Platform
	DG CONNECT	Directorate General for Communications Networks, Content and Technology
	DG MARE	Directorate General for Maritime Affairs and Fisheries
	DG MOVE	Directorate General for Mobility and Transport
	DLT	Distributed Ledger Technology
E	**EBA**	European Banking Authority
	ECSO	European CyberSecurity Organisation
	EDPB	European Data Protection Board
	EDPS	European Data Protection Supervisor
	EEA	European Economic Area
	ENISA	European Network and Information Security Agency
F	**FIDO**	Fast IDentity Online Alliance
G	**GDPR**	General Data Protection Regulation
I	**IBAN**	International Bank Account Number
	IaaS	Infrastructure as a Service
	ICS	Industrial Control Systems
	ICT	Information and Communication Technologies
	IDM	Identity Management
	IDS	Intrusion Detection Systems
	IMO	International Maritime Organization
	ISO	International Organization for Standardization
	ITU	International Telecommunication Union
J	**JRC**	Joint Research Centre (of the European Commission)
L	**LPA**	Local Public Administration
N	**NIS**	Network and Information Security
	NIST	National Institute of Standards and Technology
O	**OSINT**	Open Source Intelligence
	OT	Operational Technologies
P	**PA**	Public Administration
	PET	Privacy Enhancing Technologies

	PISP	Payment Initiation Services Provider
	PKI	Public Key Infrastructure
	PLC	Programmable Logic Controller
	PSD2	Payment Services Directive 2
	PSP	Payment Services Provider
	PSU	Payment Services User
	RTS	Regulatory Technical Standards
	RTU	Remote Terminal Unit
S	**SaaS**	Software as a Service
	SC	Smart City
	SCA	Strong Customer Authentication
	SCRM	Supply Chain Risk Management
	SIEM	Security Information and Event Management
	SME	Small or Medium Enterprise
T	**TPP**	Third Party Provider
V	**VDES**	VHF Data Exchange System

1 Introduction

One of the key features within CyberSec4Europe is to **coordinate European cybersecurity research efforts** with **demonstration cases (verticals)** in critical areas or our lives covering, but not limited to, **health**, **smart cities**, **finance**, **open banking**, **transport**, **supply chain**, **cyberattack incident reporting**, etc.

As an example of this coordination, the "**incident reporting**" vertical will pave the way to an **active dialogue with regulators** in order to reach a **harmonized EU framework for incident reporting**. This will include a certified process with an established standard classification of **work roles**, aligned with **skills** and **responsibilities**. At the same time, the advanced research techniques of this demonstration case (AI, Big Data etc.) will contribute towards the widest possible **adoption** by **relevant actors**, **cross-verticals**, and **cross-regulatory bodies**.

As another example, the "**maritime transport**" vertical will demonstrate the **ability of CyberSec4Europe participants** coming both from research and industry, to **combine their cybersecurity capacities** for a critical sector, taking into consideration generic and sector-specific security standards. The maritime transport vertical will demonstrate the **coordination, integration, innovation,** and **research capabilities** of CyberSec4Europe participants.

As a final example, "**medical data exchange**" vertical will **engage several competence centres** in order to integrate and validate, in a realistic vertical environment associated with the **Dawex data marketplace**, the research outcomes of the project. The research and technologies involved include cybersecurity and sensitive and personal data protection for medical data sharing. These outcomes provide a **common "Blueprint" of appropriate safeguards** to the industry stakeholders that manage or participate in data exchange platforms with data brokers, providers, and consumers.

VERTICAL AREAS

OPEN BANKING

SUPPLY CHAIN SECURITY ASSURANCE

PRIVACY-PRESERVING IDENTITY MANAGEMENT

INCIDENT REPORTING

MARITIME TRANSPORT

MEDICAL DATA EXCHANGE

SMART CITIES

To be able to coordinate all the different research stakeholders towards achieving the goals of their verticals, this document delivers the first integrated **Research and Development Roadmap**. The roadmap will document the important research problems that need to be addressed so as to help all verticals reach their full potential. The roadmap covers the seven vertical areas that have been defined in the CyberSec4Europe project:

- Open Banking
- Supply Chain Security Assurance

- Privacy-Preserving Identity Management
- Incident Reporting
- Maritime Transport
- Medical Data Exchange
- Smart Cities

For each of the above areas, we would like to know (i) **what the important problems are**, and (ii) **what kind of research needs to be done** in order to address these problems. To present the results in a coherent way, all individual vertical roadmaps have a similar structure that tries to address the following questions:

- Introduction
    - **Big Picture**: What is the broad setting of the vertical?
    - 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?
- 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**?

To place this work in the context of the entire CyberSec4Europe project, we should mention that it complements the efforts of Work Package WP5, which focuses on a well-defined case study (or demonstrator) for each vertical area. In contrast, WP4 takes a **holistic** (big picture) view of each vertical area, in order to build a research and innovation roadmap for both the mid- and long-term.
The rest of the document is organized as follows. Section 2 describes the context and the methodology. Sections 3 to 9 describe the roadmaps for each of the seven verticals. Section 10 describes common research areas that underlie more than one vertical and 11 summarizes our finding. Finally Annex I describes the methodology in more details and Annex II presents other roadmaps in the area of cybersecurity.

2 Context and Methodology

2.1 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.

2.1.1 Open Banking

Open banking 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.

Figure 1: Open Banking will change the way financial transactions are being carried out (image distributed under 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 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.

2.1.2 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.

2.1.3 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 really is 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.

2.1.4 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.

2.1.5 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.

2.1.6 Medical Data Exchange

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. 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.

Figure 2: Collecting and re-using medical data is expected to result in significant breakthroughs in medicine (image distributed under CC0 courtesy of https://www.pxfuel.com/en/free-photo-ebbfr)

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

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

2.1.7 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.

2.2 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?
    - 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?
- 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?

These questions are analysed in the following subsections.

2.2.1 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 wat impact

these attacks may have in their everyday lives. To illustrate this point, let us consider the following example: over the past few years we have heard about leaks of customer data which were kept on line by well-known companies[2]. 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 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 return it to normal operation. There may be some financial loss and that's all.
- 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.

2.2.2 Who are the attackers?

It is important for us to understand **who** the attackers are, what their **motives** are, and what kind of **resources** (people, money) they have at their disposal. For example, **script kiddies** have practically no resources, have little expertise and, having made some fuss, will go away. **Opportunistic hackers** may also have limited resources, and so they may do some limited damage, resulting in limited financial loss. **Organized hackers**, especially those linked to organized crime, may have more resources (possibly of the order of tens of thousands of euros), and their actions may involve major financial raids that enable them to recoup their initial investment. **Terrorists** have many resources and do not care about financial gain. At the far end of the spectrum, **enemy countries** have vast resources (hundreds of millions, if not billions, of euros and thousands of people), may do major damage, can stay undetected for quite some time, and may possibly inflict major damage on entire infrastructures (electric power grids, hospitals, water supplies, food supply chain, etc.).[3]

2.2.3 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.[4] To place the work in the appropriate context, we may divide the research

---

[2] https://www.cnbc.com/2019/07/30/five-of-the-biggest-data-breaches-ever.html

[3] For a more thorough list of the types of attackers see section I.3 on page 134.

[4] To keep the text flowing, in this section we describe only the high-level points of the methodology. More details about the methodology can be found in Annex I on page 126.

chronologically: immediate (next 12 months), short-term (until the end of the project) and long-term (after the end of the project).

3 Open Banking

3.1 The Big Picture

The revised Payment Services Directive (PSD2)[5] updates and enhances the EU rules put in place by the initial PSD adopted in 2007[6]. 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 ASPSPs 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 and PISP.

The revised Payment Services Directive (PSD2)[7] updates and enhances the EU rules put in place by the initial PSD adopted in 2007[8]. 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

---

5 Directive 2015/2366
6 Directive 2007/64/EC

7 Directive 2015/2366
8 Directive 2007/64/EC

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 ASPSPs 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 and PISP.

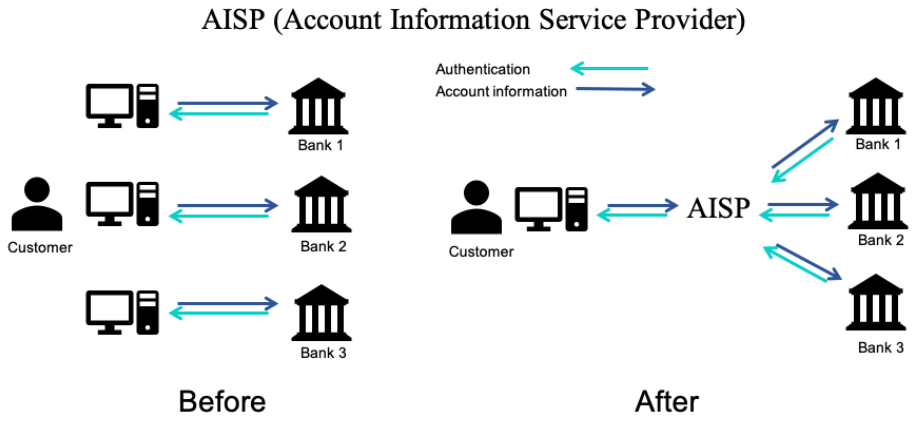


Figure 3: Account Information Service Provider

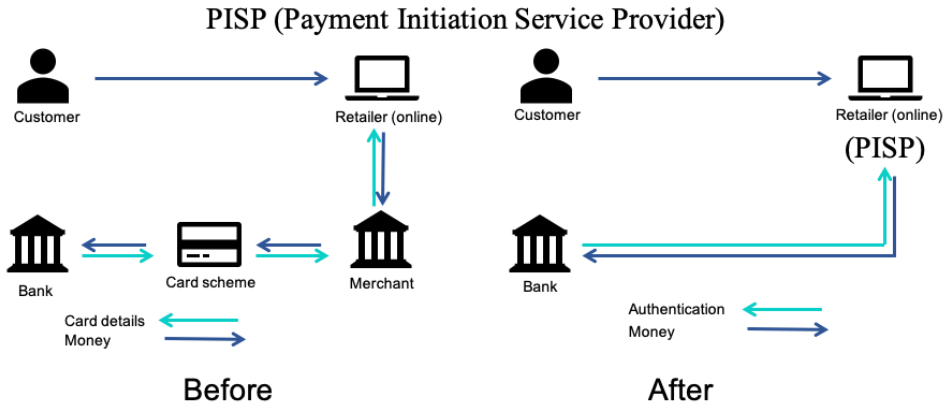


Figure 4: Payment Initiation Service Provider (PISP)

3.1.1 RTS SCA

The Regulatory Technical Standards (RTS)[9] on strong customer authentication (SCA) under PSD2 came into force on 14 September 2019. They require PSPs to adopt measures guaranteeing adequate levels of security to access and authorise remote payments, to properly operate with third parties and overall to increase the level of security of electronic payments to ensure consumer protection against fraud. Nonetheless, despite the security improvements, there remain significant 'gaps' for fraudsters to exploit.

3.1.2 PSD2 and GDPR

Although both the GDPR[10] 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[11].

Under PSD2, third parties will be able to access customer account information directly, provided they have the customer's explicit consent[12], and enable the customer to exercise their right to data portability under the GDPR.

In the payment process, there are also 'silent parties' who do not have a direct contractual relationship with the PSP, such as persons who have a bank payment account to which the PSU transfers money through the PSP[13].

---

[9] Regulation (EU) 2018/389

[10] Regulation (EU) 2016/679

[11] 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. [The interplay between PSD2 and GDPR, CMS Law-Now, April 2020]

[12] 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. [*ibid*]

[13] 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

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[14].

The link between PSD2 and 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.

3.1.3 European Data Strategy

On 19 February 2020, the EU published 'A European strategy for data'[15] 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 Act[16] and the Open Data Directive[17]: PSD2 provides the legislation on data access for payment service providers. The EC's conviction is that businesses and the public sector can be empowered through the use of data to make better decisions with the aim of creating a single European data space where personal as well as non-personal data, including sensitive business data, are secure allowing business access to *'an almost infinite amount'* of high quality industrial data. Core to this vision is the empowerment of individuals to exercise their rights through legislation and appropriate enforcement mechanisms, as is evidenced by the initiatives of MyData Global[18] and others to give individuals the tools and means

---

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. [*ibid*]

[14] 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. [*ibid*]

[15] 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

[16] Regulation (EU) 2019/881

[17] Directive (EU) 2019/1024

[18] https://mydata.org

to decide at a granular level what is done with their data. This architecture would imply the emergence of a new type of actor, the data operator, who could contribute to a new form of fragmentation of the supply chain of open banking and/or digital services, thus potentially introducing new vulnerabilities and making the current open banking security roadmap even more relevant.

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

3.1.4 Summary

All in all, there are unresolved issues, 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 startups – and offering much more choice, more transparency, lower costs, and better service to users.

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

A worldwide leading development of this Open Banking is to be found in Europe's PSD2[19] which is forcing all 4,000 banks in 27 Member States[20] 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?

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 RTS[21], Guidelines and FAQs. Also, non-PSD2 regulations, notably GDPR[22], are highly relevant and must of course be observed for any data access and use.

---

[19] 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

[20] Although the UK formally left the EU on 31 January 2020, the former Member State will remain in 'transition' until 31 December 2020, with no certainty on its future position on PSD2.

[21] European Banking Authority Regulatory Technical Standards – see Regulatory Technical Standards on strong customer authentication and secure communication under PSD2

[22] 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)

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 TPP[23] 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.

3.3.2.1 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[24]

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"[25]. Although the devices themselves demonstrate adequate security and are not themselves susceptible to attack, the increase in the

---

[23] 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.

[24] https://www.thepaypers.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=
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 approach taken by many merchants aimed at increasing online revenues and encouraging customer loyalty in a fiercely competitive market.

[25] 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

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, 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.

To progress authenticating third parties, it could be possible to use artificial intelligence/machine learning for some online operations, making it unnecessary in those cases to strongly authenticate users.

3.3.2.2 Certificate Verification

Even after the AISP (and the third party) registers with a national certificate authority, the ASPSP is not able to verify the certificate electronically, as currently the registration is not accessible. 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.

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

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

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

PSD2[26] 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.

---

[26] 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

3.3.2.4 APIs

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.

3.3.2.5 Bank Administration

A different set of security challenges is presented in the scenarios described above when the user is a corporate administrator. Although most PSD2 focus is on consumers, some of the often-neglected areas of the regulation but with high potential are the new opportunities for corporates. The special requirements of corporates[27] 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.

3.3.2.6 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.

---

[27] For example, multiple roles of authorising users, multiple signatories, authentication depending upon limits, etc

3.3.3 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.

- For the **institution** this could mean,
  - If an attacker is able to successfully carry out an attack that allows them to fraudulently siphon off the financial assets of multiple high value customers, the institution would have to make such substantial and potentially crippling compensatory payments to those customers that it would no longer be financially viable and have to go out of business
  - If a major system attack resulting in the loss of money or data or both turns out to have been the result of significant negligence on the part of the institution, and if the institution is not able to contain the resulting media exposure, it would have such an impact on the brand and reputation of the institution that it might not be able to recover.
  - It is a well-documented phenomenon, that, after one successful attack, an attacker who remains undetected goes on to carry out further attacks at other institutions over the following weeks and months[28]. 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 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

[28] 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

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 mindset, 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 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);

JRC Cybersecurity Domain: Security Management and Governance

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

JRC Sectorial Domain: Financial

- Banking services

3.5.2 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

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

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

- **Legislation:** Different national competent authorities have differing licensing regimes[29] and different courts have different interpretations of legislation, primarily, but not exclusively, associated with PSD2.
- **Protocols and APIs:** Italy's RI.BA[30] and Bolletino payment schemes use different protocols to those of iDeal[31] in The Netherlands. and different banks offer different APIs which could be based

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

[30] 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)

[31] 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.

on the those proposed by, for example, the Open Banking Implementation Entity (OBIE)[32], the Berlin Group[33], STET[34] 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;
- 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;

---

[32] 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.

[33] 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.

[34] 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.

JRC Sectorial Domain: Financial

- Banking services

3.5.4 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

3.5.5 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

3.5.6 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.

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 set, five or six, 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 al[35]. In addition, it is vital that a common European approach to harmonising standards is taken to a global level, principally with FAPI[36] 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. Startups 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.

Tools: A number of tools address different aspects of this challenge: 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)

---

35 These include similar initiatives such as those in Poland, Slovenia and France.

36 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.

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

Mechanism: The approach requires the ability to carry out a series of real time actions on encrypted personal banking-related data, ideally 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 1: 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	To simplify the user experience in using open banking user-oriented interfaces and tools without loss of functionality

		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)	
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 initial exercise should be to ***map the whole Open Banking process end-to-end***, drawing a map of all the stakeholders involved, how they interact, how they rely on each other and how the chain of trust is 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 3-year (or until the end of the project) plan

Until the end of the project, we should investigate the ***impact of the discontinuation of relationships in an established trust chain across the various scenarios*** envisaged in the 12-month plan. We should also investigate 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.

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 eIDAS[37] certificates*** (with seals and transport certificates as required by regulation) with emerging PSD2-specific directory services
- Old "credential sharing" and "screen scraping" technologies (as permitted in PSD2 regulation under certain circumstances) versus modern methodologies (two-factor/SCA) and ***modern cyber-attacks*** (especially man-in-the-middle)
- Role of ***mobile ecosystem*** (apps, authentication, biometrics, wireless data, etc.) in PSD2 security
- Issue of ***"consent" under GDPR within PSD2***: roles/liabilities of actors, conflicts between privacy and payment regulations, need for separate/neutral consent platforms at neither bank nor TPP
- ***Risks in the planned next steps*** in Europe, especially the API "scheme" and new "rich POS solutions" triggering instant credit transfers (with irrevocable fund transfer and limited time to do full AML/KYC/FATCA/sanction checks) at physical and virtual e-commerce and m-commerce checkouts.

[37] 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

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 sale 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 transporting and tracing the location of all components and goods, guaranteeing the quality and integrity of all parts and products, accrediting the technical and organizational competence of all stakeholders, and identifying and resolving potential issues or conflicts. Moreover, we need to consider that supply chain ecosystems are highly heterogeneous, as the complexity and requirements in the management of all goods (from bicycles to planes, from web software components to power plant software architectures) are different.

The supply chain ecosystem is also evolving due to the integration of information technologies (IT) with the existing operational technologies (OT) infrastructures. The integration of these new "digital and ICT" 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, providing 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 are one of the core foundations of our modern society. Not only our economies, but also our daily lives depend 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. 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 these multiple standards and reports. Note that this taxonomy takes into consideration the dual nature of existing supply chains, where the **goods** that are managed and processed within the supply chain can be either physical or digital, and where data and algorithms – which are used to build the software – are the equivalent of raw materials and production processes in a software supply chain.

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

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

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

As for the **assets** that comprise the supply chain ecosystem, 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, RFID labels…), *IT Networks and components* (facilities networks, supply chain collaboration networks, network components). *OT Systems and Networks* (e.g. Industrial control systems), *OT End-Devices* (e.g. sourcing and processing machinery, manufacturing machinery, cargo handling systems), *Safety and Security Systems* (e.g. detection and alerting systems, access control systems), *People* (including internal and external staff), and *Information and Data* (e.g. intellectual property, transport data, enterprise agreements).

4.3.2 What is expected to go wrong?

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

- General threats:
    - Sabotage (both physical and digital), cascade effects, export control violations, overall corruption, service disruption, insider threats (both physical and digital)
- Specific goods threats:
    - Tampering with goods (including packaging and labelling), 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

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

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

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 NIST [NIST 2012] and identified in the supply chain case are the following:

- Harm to Operations:
    - *Inability to perform current missions/business functions*: attacks through the supply chain become commonplace, and organizations are always vulnerable.
    - *Inability, or limited ability, to perform missions/business functions in the future*: as organizations are always vulnerable, it becomes impossible to fully recover from continuous attacks.
    - *Harms (e.g. financial costs, sanctions) due to noncompliance*: complex regulations cannot be implemented.
    - *Relational harms*: Trust relationships between organizations are lost, because managing the supply chain threats has become an impossible task.
- Harm to Assets:
    - *Damage to or loss of physical facilities*: terrorist attacks take advantage of supply chain vulnerabilities to damage physical facilities, also causing human casualties.
    - *Damage to or loss of information systems or networks*: traditional cyber-attacks, such as ransomware, relentlessly disable the underlying IT infrastructure that supports the supply chain ecosystem.
    - *Damage to or loss of component parts or supplies*: it becomes impossible to manage the threats against physical/digital assets when the supply chain is transformed into a chaotic supply web.
    - *Damage to or 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 stated in Section I.3 have targeted supply chain scenarios. In particular, *criminal organizations* have focused mostly on the smuggling of people[38], weapons, and illegal substances[39] [40], theft[41], and various digital threats such as digital skimming[42] and theft of personal information[43]. *Terrorists* have also tried to abuse the supply chain to perform acts of terror[44]. All *intelligence services* have also participated in the manipulation of the products and services of the supply chain[45], including the software supply chain[46], for various purposes such as personal and industrial espionage and sabotage. Last but not least, various *supply chain actors* have also acted as insiders, causing problems in the supply chain due to product manipulation / mismanagement[47].

[38] 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
[39] https://www.bbc.com/news/world-europe-25640485
[40] https://www.bbc.com/news/world-europe-24539417
[41] https://onlinelibrary.wiley.com/doi/pdf/10.1111/deci.12336?casa_token=ifPZDxYdAwQAAAAA:jU0gYtsIT0fFOlOT3V5ozqHZQrrQW328jTZsVuK16QCQhBuSPFAeasxZtfSkqVQQ1enFvcBHASnXFXE
[42] https://blog.trendmicro.com/trendlabs-security-intelligence/new-magecart-attack-delivered-through-compromised-advertising-supply-chain/
[43] https://research.checkpoint.com/2019/operation-sheep-pilfer-analytics-sdk-in-action/
[44] 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
[45] https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies
[46] 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
[47] https://www.theguardian.com/uk/2013/feb/15/horsemeat-scandal-the-essential-guide#101

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 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 matrixes 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 to foster 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.

4.5.2 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.

4.5.3 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.

4.5.4 Challenge 4: Management of the accreditation of supply partners

Another aspect that is widely considered in existing recommendations and standards concerns the diverse procedures for the certification and accreditation 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 accreditation processes pose various challenges. One is the complexity of the accreditation 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 accreditation 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 accreditation 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 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 accreditation of supply partners. Another main process reviewed in the supply chain big picture is the accreditation 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 accreditation 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 CORAS[48].

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 A, B defined in Section 0, 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

[48] http://coras.sourceforge.net/

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.

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 PLEAK[49], 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 accreditation 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:

[49] https://pleak.io/home

- 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 2: 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
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

One of the main challenges related to the protection of supply chains involves the ***protection of IT/OT infrastructures and networks***. At present, there are already various security and privacy mechanisms in areas such as secure communications, secure data storage and real-time detection, which can be combined

to provide an adequate level of protection for these infrastructures. In addition, approaches such as *penetration testing and software analysis tools* can be used to monitor whether the security of the infrastructure is being maintained. For the development of security and privacy solutions that cater to the specific needs of a supply chain ecosystem, we mainly need to apply or adapt existing security tools rather than developing them from scratch. Nevertheless, note that even if these security and privacy mechanisms are available within the next 12 months, their deployment and integration in existing supply chain infrastructures will surely take much longer than 12 months.

Other aspects that can be studied and developed within 12 months are mainly related to the ***integration of blockchain-based solutions*** into supply chains. In fact, we need to consider that there are already various platforms, pilot programs, and even commercial products that are running supply chain processes over various blockchains and benefiting from their advantages. Therefore, it will be possible to analyse, develop, and deploy certain mechanisms that take direct advantage of the tenets of the blockchain, such as the *registration and sharing of supply chain events between authorized parties.*

4.8.2 3-year (or until the end of the project) plan

The protection of the IT/OT infrastructure of supply chains can be further improved in three years' time. For example, ***the availability of lightweight distributed detection mechanisms*** can facilitate the integration of proactive defence mechanisms in supply chain infrastructures. Other services, such as the ***provisioning of shared data spaces***, can be available within this time frame. From the point of view of one entity, the *deployment of security- and privacy-oriented solutions based on information policies* can limit both the amount and the granularity of the information that can be shared in the data space. Moreover, these information policies can make use *of available identification frameworks for federated ecosystems*, which will facilitate the exchange of information between interested parties.

Another aspect that can be properly studied in 3 years ***is the application of existing supply chain risk management programs, and the development of various applications that facilitate their automation***. Even though self-healing mechanisms might not be made available within three years, the output of these automation programs can be used by human operators to update the protection against unforeseen situations and new threat vectors.

Regarding the 3-year plan and the integration of blockchain-based solutions, we have to point out that, while in 3 years it will not be possible to truly manage the whole complexity of the existing web of supply chain over the blockchain, it is almost certain that ***various security and privacy tools based on the blockchain will be available***. Those include the deployment *of smart contracts to monitor supply chain exceptions, the availability of self-sovereign identity solutions, and the exchange of private data through various means* (private blockchains within other blockchains, private documents backed by hash values).

4.8.3 Beyond the end of the project plan

As for 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, and a deeper integration with existing frameworks, such as compliance requirements and clearance processes.

Another aspect to take into consideration ***is the availability of self-healing processes combined with other tools, such as threat intelligence sharing,*** which will have multiple uses: from the *automatic hardening of the supply chain IT/OT infrastructures and networks to the continuous deployment of better security and privacy policies*, including more advanced solutions such as *data recovery*. However, the challenges associated with this goal are numerous, and involve not only one but multiple supply chain partners.

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 said services or 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 identity because an issuer in which it trusts attests them.

Thus, the key process in identity management is the authentication/authorization, where users gain access to some service or resource by proving that they meet the required conditions to the service provider. It may be preceded by an issuance process, where an issuer (or multiple) gives the users the attestations necessary to proof their identity. In these processes, different components are involved, like the issued attestations (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 same certificates, 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) [Cambell 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 [Truman 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 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 (General Data Protection Regulation) [Paul 2017], some providers do not follow a good protocol in order to ensure the security of personal data and might, either through negligence or financial motivation, leak 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 [Bernabe 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 eIDs) that would provide sufficient trust.

5.3 What is at stake?

5.3.1 What needs to be protected?

Services and implementations. A (privacy-preserving) identity management system involves a variety of parties, including issuers, relying parties, potential authentication service providers, as well as users. The security of the entire system rests on the security of its weakest link, as a compromise of either participant can cause a negative impact on all other entities in the ecosystem. Thus, secure protocol designs, implementations and deployments are needed.

Access to key material. Related to the above, access to any type of secret key material of any party (encryption keys, credentials, signing keys, etc.) can subvert the security of the entire system. Access to all secret key material thus needs to be protected by physical (e.g. hardened devices) but also logical (e.g. security architecture) means.

5.3.2 What is expected to go wrong?

Below, we summarize the main threats and security risks in the context of privacy-preserving authentication. For further reading, we refer, e.g., to ENISA[50].

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, misprotection 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 protocol design may enable users to undermine the authenticity of the authentication process. In this case, malicious users can successfully authenticate without having access to valid authentication data such as cryptographic key material, biometrics, etc. As a result, an attacker may either consume a service illegitimately or gain access to another user's account.

Subverting business models. Depending on the protocol design, its implementation, and whether or not authentication is bound to a hardware token (e.g. a trusted platform module), it may be possible for users to share their accounts. In particular, this is a risk if users do not need to share their entire, e.g., credential or key material, but can perform single authentication sessions on behalf of another user. For instance, if user A wants to authenticate in a challenge-response based scheme, he/she might forward the challenge to user B (holding a valid authentication token), receive the response to 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 being noted 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 users.

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 filtered 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.

---

[50]ENISA: "Mobile Identity Management ", 2010. Available at https://www.enisa.europa.eu/publications/Mobile%20IDM

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), to maliciously invalidate a user's credential.

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. We here 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/external). 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 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.
- S***toring (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

5.5.2 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

5.5.3 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

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)

5.5.4 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)

5.5.5 Challenge 5: Password-less authentication

Most web applications have authentication process that rely on the password paradigm. It is evident that a password can be considered secure when it contains 20 characters or more, is complex (is comprised of alphanumeric characters, symbols and non-dictionary words), is only stored in the brain of the user, is used only in one application and is changed frequently. As the number of accounts each user maintains has greatly increased in the last few years, users are having a hard time memorizing and managing all these passwords. To solve this password overload problem, users have come up with solutions that directly affect the security of their accounts and the privacy of their data; they either simplify their passwords to be easy to remember, or reuse the same password on different services, or store their passwords in a "secure" place, on paper or using a password manager. At the same time, passwords are targets of multiple attacks, as they can be leaked, key-logged, replayed, eavesdropped, brute-force decoded and phished.

Relevant Research Goals

- ***Development of password-less authentication solution***; in this context, the need to employ a secure and user-friendly password-less authentication solution has emerged. To be widely used, the solution should be easily adoptable by both end-users and service providers, as well as allowing integration with privacy-preserving identity management solutions, such as Idemix.

JRC Cybersecurity Domain:

- Identity and Access Management
    - Identity and attribute management models, frameworks, applications, technologies, and tools;
    - Protocols and frameworks for authentication, authorization, and rights management;
    - Authentication/Access Control Technologies (biometrics);

    - Privacy and identity management;
    - Identity management quality assurance.
- Human Aspects
    - Enhancing risk perception;
    - Usability;
    - Automating security functionality,
    - Privacy concerns, behaviours, and practices.

JRC Sectorial Dimensions:

- Safety and Security
- Digital Services and Platforms

JRC Technologies and Use Cases Dimensions:

- Information systems
- Critical infrastructures Protection
- Disaster resilience and crisis management
- Blockchain and Distributed Ledger Technology (DLT)
- Human Machine Interface

5.6 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).

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 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) proposed by the FIDO Alliance [FIDO2015]. The main challenge objective is to implement and deploy 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 protocols, such as FIDO UAF.

Table 3: 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

5.8 Roadmap

5.8.1 12-month plan

5.8.1.1 Unlinkability and minimal disclosure

To address this challenge, there is a 12-month plan whose final goal ***is the implementation and deployment of a P-ABC system that meets the requirements of unlinkability and minimum disclosure***. Taking advantage of existing implementations, such as Idemix, during the first months (1-3), a basic deployment will be carried out that allows simple testing over known use cases, such as user age-proofing during a commercial transaction. During the following few months (4-8), we will seek ***to improve the system in***

terms of usability and efficiency, applying it in complex contexts with the main objective of increasing its adoption by users and service providers.

Finally, during the last few months, ***the solution may be evaluated in terms of simplicity, performance and the satisfaction*** of the involved actors by the deployment of various proofs of concept.

5.8.2 3-year (or until the end of the project) plan

5.8.2.1 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.***

5.8.2.2 Distributed oblivious identity management

To address this challenge, there is a 3-year plan where the final goal is the ***deployment of a distributed oblivious identity management system that fulfils the security and privacy requirements.*** In this plan, several activities are contemplated. The first step would be to establish well-defined requirements for the system and to define the use cases that will be used for testing it. Then there are tasks involving the design of the system architecture, development of cryptographic components and framework integration. The development of these tasks will be iterative, and it is expected that ***two reference implementations of the system*** (at around half the planned time and near the end of the project) ***will be obtained and used for testing.*** In addition, pilots for the use cases will be deployed and used to evaluate user experience and compliance with legal requirements.

5.8.2.3 Privacy preservation in blockchain

During the development of a privacy-preserving solution applicable to blockchain it is necessary to achieve different objectives separately. First, select and test the necessary cryptographic technologies that are sufficiently light, secure and integrable with one of the existing blockchain solutions (e.g. Hyperledger). In this sense, the selection of the blockchain platform is also relevant, as an erroneous or inadequate choice could make the integration difficult or even impossible. Therefore, during the first year the possibilities of the various ***cryptographic technologies and the available blockchain infrastructures should be systematically tested*** so that the best pair of them may finally be chosen.

Once the starting points have been selected, the next step would be to ***adapt both technologies to work together***. Initially, a basic integration that would provide a primitive support, followed by an extension of the possible functionalities with respect to the privacy to be achieved. In addition, concrete use cases should have been identified that would allow the evaluation of the proposed solution.

At the end of the second year and the beginning of the third, there should be an ***implementation*** mature enough to begin testing ***with proof of concepts to demonstrate the main functionalities***. Finally, during the third year, the ***full integration*** should have been 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.

5.8.2.4 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***. To address this challenge, a 3-year plan has been created. For the next year, the authentication system's requirements should be thoroughly studied and the architecture should be designed. Then, a comparison should be performed between the different FIDO UAF versions to find the most appropriate. The second year will be entirely devoted to the prototype implementation and deployment of the password-less authentication solution. Finally, during the third year, the integration with the privacy-preserving identity management system should have been finalized in order to initiate the security and performance analysis and evaluation of the system. In parallel with the evaluation, the pilot usage of the system should begin for the user experience testing process to take place, as usability is regarded as a very important attribute for an authentication system.

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, 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 PSD2[51] (Payment Service Directive 2), the ECB SSM[52] (European Central Bank Single Supervisory Mechanism) and the T2[53] (Target2) mandatory incident reporting requirements. There are therefore mandatory incident reporting requirements arising from the EU legislation, but also from the individual national regulatory frameworks and from other mandatory requirements established in the single member states by the national competent authorities. On top of this, to fulfil the BIS-IOSCO Guidelines[54] (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

[51] 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

[52] https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html

[53] https://www.ecb.europa.eu/paym/target/target2/profuse/nov_2018/shared/pdf/Information_Guide_fo_TARGET2_users_v12.0.pdf

[54] Guidance on cyber resilience for financial market infrastructures. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf

e-IDAS[55] (electronic identification and trust services), GDPR[56] (General Data Protection Regulation) and NISD[57] (Directive on Security of Network and Information Systems), whose applicability is cross-sectorial, and all introduce their own requirements, with their scope, templates, and timelines.

Indeed, just considering the example of the NIS Directive, the same mandatory incident reporting process is applicable to the operator of essential services (OES) and to the digital service providers (DSPs), which implies that the incident reporting framework also applies to other industries in addition to the financial sector: energy, transport, health, drinking water supply and distribution, and digital infrastructures.

OES and DSPs have to fulfil the requirements according to the rules established under the NIS Directive as defined by the designated national competent authority in the relevant member state(s). Since most of the regulatory requirements that arise under directives might be transposed in a different way across the member states, the mandatory incident reporting process becomes even more complex for those entities that operate across multiple jurisdictions.

ENISA[58] 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.

[55] 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
[56] 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)
[57] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016.
[58] 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)

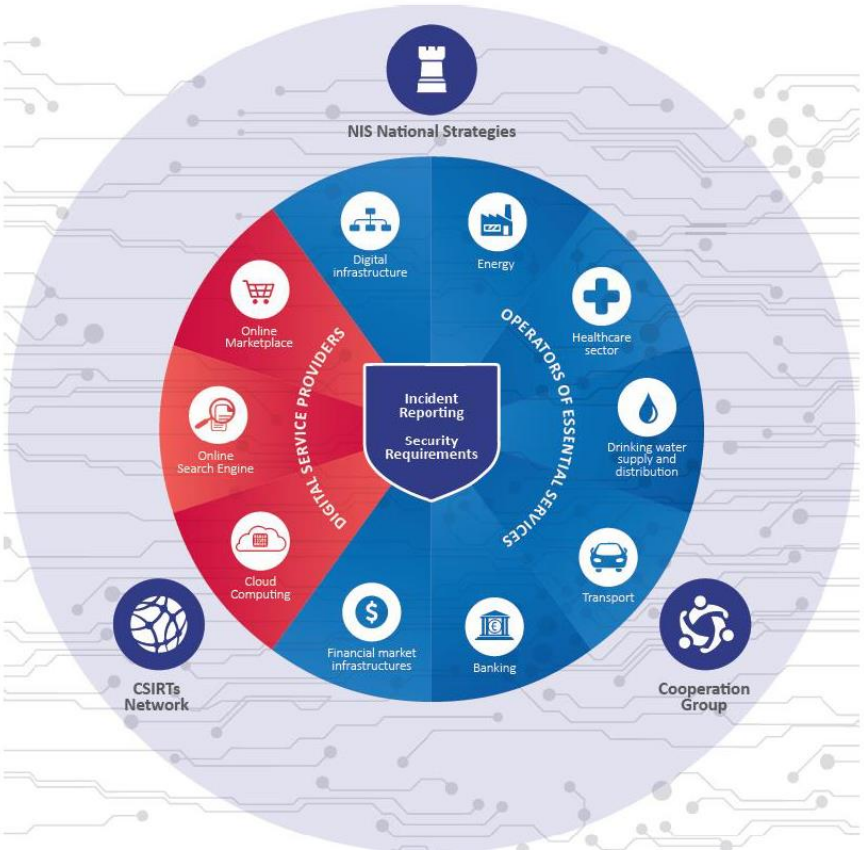


Figure 5: Graphical overview of the NIS Directive. Source: Incident notification for DSPs in the context of the NIS Directive[59]

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.

[59] 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.[60].

It is worth mentioning that in their recent joint advice[61], 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.

---

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

[61] *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 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 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

6.5.2 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

6.5.3 Challenge 3: Promote a collaborative approach for sharing incident reports to increase 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 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.

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

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 Cyphon[62], TheHive[63] or Fast Incident Response (FIR)[64].

[62] https://www.cyphon.io/
[63] https://thehive-project.org
[64] https://github.com/certsocietegenerale/FIR

6.7.2 Incident Impact Assessment

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 be skipped (at least during Roadmap 1).

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

6.7.4 Incident Data Collection

In the context of task 3.4 different tools based on the MISP[65] 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).

[65] https://www.misp-project.org/

Table 4: 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, Reliable-CTIs - Reliable Cyber-Threat intelligence sharing, TIE - Threat Intelligence Integrator (D3.1, Section 5.3)	Mechanisms to improve trustworthiness and reliability for threat intelligence data sharing using MISP and qualification of IoCs to improve actionability.

6.8 Roadmap

6.8.1 12-month plan

During the next 12 months, we will focus on Challenges 1 and 2 to provide a ***prototype of an incident reporting platform*** that helps the incident reporting teams of financial institutions to fulfil the requirements of the mandatory incident reporting to the Supervisory Authorities, in particular under PSD2 and ECB regulatory frameworks. As far as we know, and as it has been also stated by the financial institutions participating in the demonstration case (Intesa Sanpaolo and BBVA), currently there are no available commercial/free platforms implementing the actual incident reporting process fitting their requirements and covering the whole lifecycle of the incident, and in particular focused on security related incidents in the financial sector. Taking into account all the requirements, we carefully analysed different groups of tools in the context of incident management and response (i.e. Cyphon, TheHive, Fast Incident Response- FIR, GRR Rapid Response and MIG: Mozilla InvestiGator), issue tracking systems or ticketing systems (i.e. RTIR: Request Tracker for Incident Response, osTicket and Open Technology Real Services) and pen-testing reporting tools (i.e. Dradis, MagicTree and Metagoofil) among others, with the objective of identifying and evaluating the existing solutions. As a result of this analysis, we concluded that none of them was able to fulfil the requirements identified in D5.1, and consequently we selected one available open source incident management tool, TheHive (which does not include incident reporting capabilities, only incident management), and we decided to extend it (using CS4EU WP3 assets and specific configuration/templates in TheHive) to support mandatory incident reporting workflow in the financial sector under different applicable regulations. Consequently, we will work on the deployment of tools (WP3 assets and adaptation of available open source tools, in particular the incident management and response tool TheHive) to provide the following features: data collection of all information required for the mandatory reports (in particular, for M12 only for the First Initial Report required according to ECB and PSD2 regulations) through a graphical interface, evaluation of the event impact severity and the Competent Authorities that need to be notified (just a basic evaluation under specific criteria defined in ECB and PSD2 regulations for demonstration purposes, because there is no WP3 asset covering this functionality as it was included in the requirements identified in D5.1), enforcement of a workflow with managerial judgement to have approval to proceed with the preparation of the reports, and generation of the actual reports in the required format (Excel files) populated with the information collected.

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

Until the end of the project, we will improve the incident reporting platform addressing Challenge 3 with the ***integration of threat intelligence information*** shared through MISP and extending the number of regulatory frameworks supported by the platform. In particular, the idea is to include the following:

- Personal Data Breach notification under GDPR,
- Incident Reporting for Operators of Essential Service under NIS Directive,
- Incident Reporting for Target2 participants
- Incident Reporting for Trust Service Providers under eIDAS regulation.

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.

- **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.

7 Maritime Transport

7.1 The Big Picture

The Maritime Transport is a complex activity, engaging all the structures, modes and equipment required for the carriage of passengers or goods via sea, that constitutes the shipping trade (seaborne) or else passengers and cargo shipping, 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 "an 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 cornerstone of the maritime transport and logistics industry are port communities. Vessels are the maritime transport means to conduct the seaborne transport operations. Autonomous ships are seaborne vessels that transport freight over navigable waters without or with mere human interaction. Maritime transport enfolds 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 considered the passenger transport, LNG (liquefied natural gas) transport, container cargo service, dry and bulk cargo service, route planning, vessel traffic service, etc. 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 8.3.

Maritime transport services are implemented through maritime Critical Information Infrastructures. Indicative Maritime transport infrastructures are considered 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, ERPs, etc.. 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.

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 6. 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.

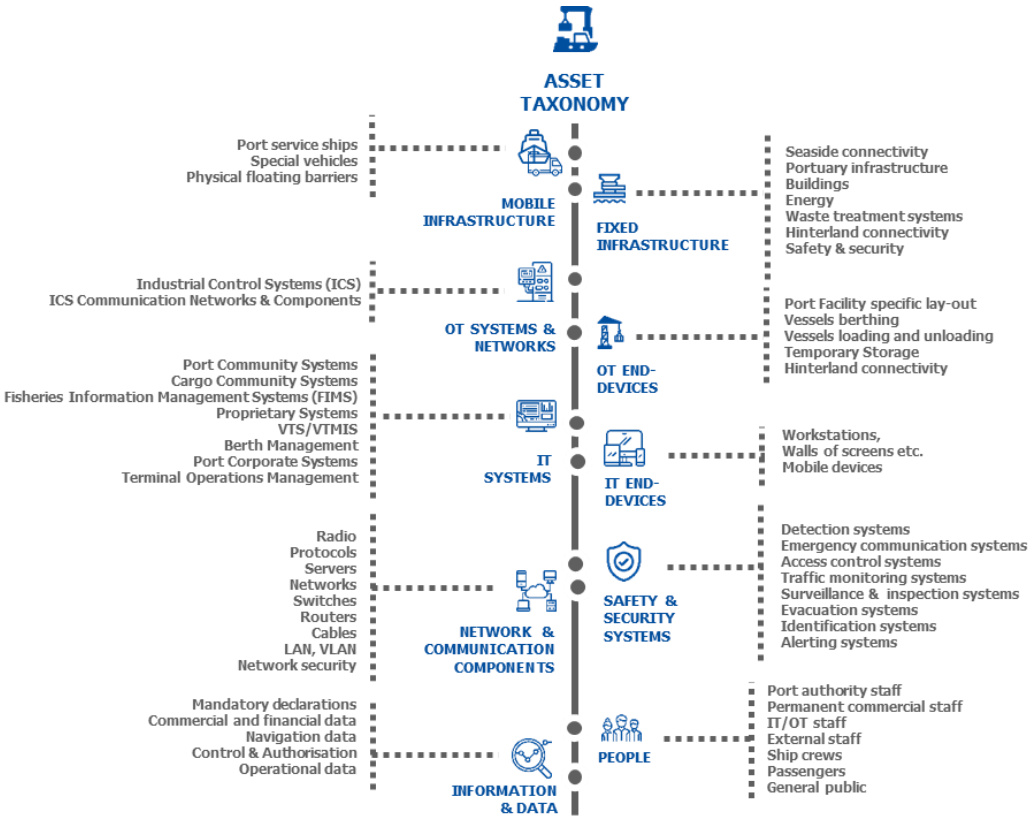


Figure 6: The ENISA taxonomy for the critical maritime assets

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 7. 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, the components of which are briefly described below [AGK 2019]:

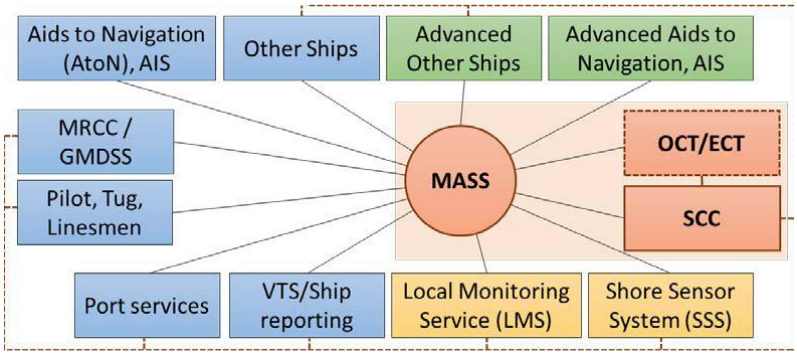


Figure 7: Context diagram for autonomous ship operation [RN 2017].

- **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 [RT2014], 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. in the Port of Maersk, the Port of Barcelona US Ports (Long Beach, San Diego), Austal, Royal Navy of Oman. ENISA [ENISA 2019] has provided the following maritime cyber threat landscape:

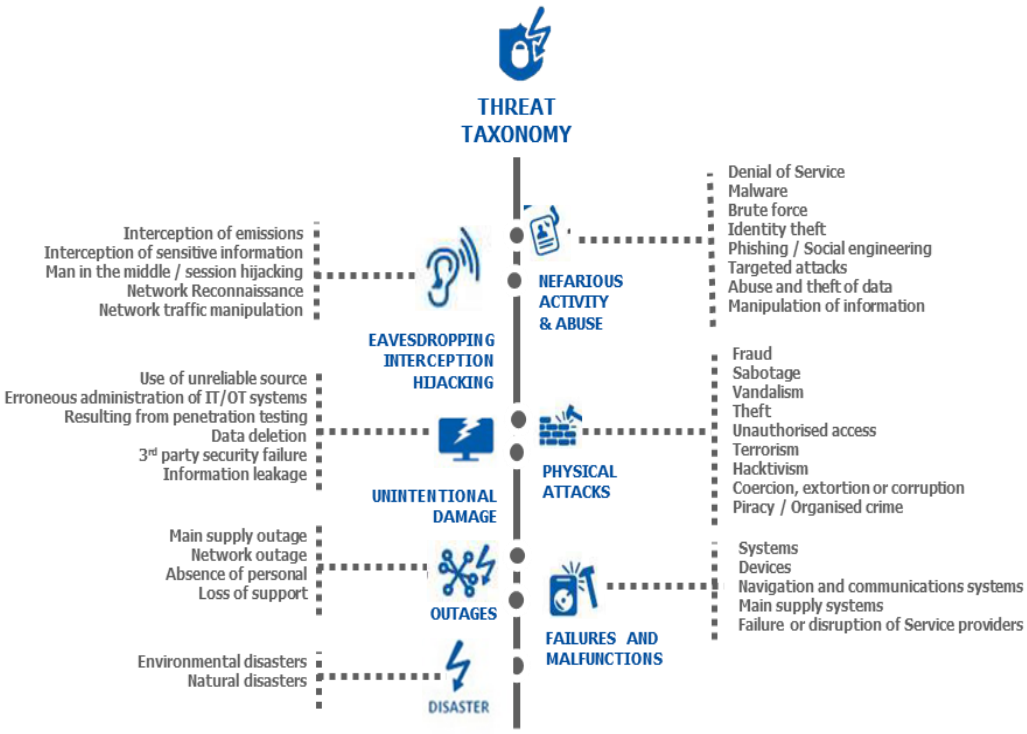


Figure 8: The ENISA threat taxonomy for the maritime transport sector [ENISA 2019]

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 l**ack 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 (Annex I) 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 (Annex I) 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 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

7.5.2 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

7.5.3 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

7.5.4 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 ITU standard, work still remains to be done to protect the application data that is being transferred over this communication channel.

Specific Research Goals

- ***Develop wireless access control mechanisms through secure channels, to be utilized in cases where remote intervention is required on vessels.*** As the possibility for remote intervention is a clear function

requirement, wireless access control mechanisms based on secure channels are a necessity, in order to enable such functionality.

- ***Design and develop trust infrastructures that take into consideration the environmental limitations of the maritime transport sector, such as the network availability and the communication costs.*** Since stability of communication is an issue, it is crucial to facilitate the availability and stability of the communication solutions. As such, the solutions need to be scalable and redundant.
- ***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

7.5.5 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 [LGPP 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] [HOMRJ 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 [Ferreira et al, 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 CS4E 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 7.5.1.

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 [L 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].

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. [Pawloski et al, 2017] [van der Veen et al, 2016] [Sarbinowski et al, 2016] [Clang10]) for critical maritime infrastructures, as described in the relevant challenge (see Section 7.5.2).

7.7.4 Secure Maritime Communications

As argued in association with research goal 4 within Challenge 8.4.4, 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 5: Challenges identified in the Maritime Transport Vertical and Tools needed to address them

Challenge	Tools required for	Tools contemplated for Maritime Transport	Tools/Methods that need to be addressed
Challenge 1	Early identification and assessment of risks, threats and attack paths for critical maritime systems	Collaborative Risk Management methodologies and risk assessment tools, such as MITIGATE (D3.1, Section 5.4), CORAS (D3.1, Section 5.2) and BowTie Plus (D3.1, Section 5.2)	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). Development of stable data sets for the maritime environment. 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.
Challenge 2	Security hardening of maritime infrastructures, including cyber and physical systems	TypeArmor (D5.2, Section 6.2) and VTPin (D5.2, Section 6.2)	Software analysis and identification of unsafe components. Provide security controls at the compiler level, and runtime security mitigations. Utilize binary-level analysis techniques and methodologies for program hardening with no recompilation. In addition, entirely program-agnostic techniques that are will be explored, such as pre-loading the binary with secure memory.

Challenge	Tools required for	Tools contemplated for Maritime Transport	Tools/Methods that need to be addressed
Challenge 3	Resilience of critical maritime systems	MITIGATE (D3.1, Section 5.4), CORAS (D3.1, Section 5.2), BowTie Plus (D3.1, Section 5.2), PKI service (CySiMS) (D3.1, Section 7) and Secure AIS ASM endpoint (D3.1, Section7)	Develop and implement monitoring techniques that will analyse the data, and vulnerability databases providing efficient indexing. Explore, map and address risks related to unwanted maritime security events through the generation of bow-tie diagrams.
Challenge 4	Maritime system communication security	PKI service (CySiMS) (D3.1, Section 7), Secure AIS ASM endpoint (D3.1, Section7) and BowTie Plus (D3.1, Section 5.2)	Development of a targeted trust infrastructure. A PKI service provision to support encryption requirements to safeguard data AIS and VDES communication.
Challenge 5	Securing autonomous ships	PKI service (CySiMS) (D3.1, Section 7), MITIGATE (D3.1, Section 5.4) and BowTie Plus (D3.1, Section 5.2)	Model threats against securing maritime autonomous surface ships (MASS). Develop risk models capable of addressing heterogeneous part of autonomous ships.

7.8 Roadmap

Based on the analysis of the relevant research challenges for maritime transport cybersecurity identified in section 7.5, and on the survey of the existing methodologies and tools, both within and outside the scope of CyberSecurity4Europe, the following research roadmap is defined.

7.8.1 12-month plan

In the course of the next 12 months of the project the research goals to be achieved are the following:

Concerning the research challenge described in Section 7.5.1 **(**Challenge 1: Early identification and assessment of risks, threats and attack paths for critical maritime systems**):**

- We plan to work on ***developing methodologies and tools to procure stable datasets*** that are related to: (i) targeted threats and vulnerabilities specific to the context of critical maritime systems and (ii) targeted threat models that will be able to capture threat agents and complex threat events, such as cascading, cumulative and common cause threats. Using those datasets, neural networks can be trained to predict vulnerable attack paths by identifying a set of characteristics when scanning new systems.

Concerning the research challenge described in Section 7.5.2 (Challenge 2: Security hardening of maritime infrastructures, including cyber and physical systems):

- Our goal is to work on methodologies and tools for ***software analysis and identification of unsafe components*****.** As discussed above, in the maritime sector highly customized software may be used. Thus, current software analysis tools must be enhanced to perform tasks like the identification of the programming system used for implementing a particular program, the identification of possible security controls at the compiler level, or the existence of runtime security mitigations.

Concerning the research challenge described in Section 8.4.4 (Challenge 4: Maritime system communication security):

- Our short-term goal is to ***design a trust infrastructure targeted to the maritime environment***, having in mind constraints such as limited bandwidth, the communication latency and the cost of the communication. Such infrastructure will facilitate the preservation of entity authentication, communication integrity and confidentiality of maritime communications. As the common incidents in the maritime sector are associated with interception attacks, it is crucial to have solutions that support communication not being exposed to intruders and not being compromised.

7.8.2 3-year (or until the end of the project) plan

In the course of the next 3 years the research goals to be achieved are the following:

Concerning the research challenge described in Section 7.5.1 (Challenge 1: Early identification and assessment of risks, threats and attack paths for critical maritime systems):

- We plan to ***design efficient cyber-attack path discovery algorithms*** that are capable of capturing the dependencies and interactions of maritime systems. Such algorithms may require the use of novel machine learning algorithms that will support the dynamic identification of possible attack paths, as

well as their assessment in terms of risk. In addition, we plan to enhance existing risk assessment methodologies with ***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. Finally, another goal is to ***visualize vulnerable attack paths and attack patterns.***

Concerning the research challenge described in Section 7.5.2 (Challenge 2: Security hardening of maritime infrastructures, including cyber and physical systems):

- Under this challenge, our research plan is to work on ***program hardening with no recompilation.*** Since in the maritime sector, it is very likely that the source code of existing software will not be available, ways of protecting binary-only programs must be explored. In addition, another goal to be met is ***hardening programs without modifications.*** Protecting binary-only programs is fairly challenging; nevertheless, there are cases when highly custom 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 will be explored, such as preloading the binary with secure memory.

Concerning the research challenge described in Section 7.5.4 (Challenge 4: Maritime system communication security):

- In this context we aim to work towards the ***development of 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 communication solutions. As such, the 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 7.5.3 (Challenge 3: Resilience of critical maritime systems):

- ***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 7.5.5 (Challenge 5: Securing autonomous ships):

- 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.

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 enormous amount of data. On the other hand, when companies and public organizations (health, education, legal, etc.) provides online services, they require and generate massive quantity of data. In both cases the trend is to grow more. In the case of the health domain, a huge amount of data is generated year by year, reaching around 10 petabytes (PB) per year[66]. This enormous amount of stored data can be used by their producers (individual citizens, wearable companies, hospitals, health organizations, pharma laboratories) improving citizens health. The value of this information increases when is shared with others. A medical data exchange platform can sharply increase the value of these data, gathering data providers and data consumers in a single place. Additionally, the possibility of cross-border exchange of data, due to the increase of cross-border businesses gives an added value to these data.

Different kind of data (financial, statistic, scientific, education, personal or health data) can be stored and shared between parties. Health data is a kind of sensitive data that must be managed with special care. The management and access to these sensitive data on the data exchange platforms need to be appropriate in terms of quality, security and privacy. The medical data exchange platform must assure the integrity and reliability of the data. Additionally, only allowed users will get access to the platform where the data or metadata are stored. Also, the data must be protected at any moment when transiting between parties. Moreover, during the sharing process the user data privacy must be preserved at any moment. Furthermore, in order to engage new users to the platform willing to share and consume data, both the data consumers and data providers must interact with the exchange platform in a friendly way. Finally, the platform must fulfil with the current legislation assuring the user rights and the data protection accomplish. These measures will prevent a third party to learn from user data, providing a secure and smooth use of the medical data exchange platform. In the context of Medical data exchange demonstrator these aspects will be addressed.

8.2 Overview

According to Forbes[67] more than 2.5 quintillion bytes of data were created each day during 2018; 463 exabytes of data per day are expected in 2025[68]. Data assets in healthcare domain are growing fast than in other sectors[69]. 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%[70].

---

[66] https://www.dellemc.com/en-tz/collaterals/unauth/briefs-handouts/solutions/h17823_solution_brief_driving_real_clinical_business_outcomes_with_a_modern_it.pdf
[67] https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/
[68] https://www.raconteur.net/infographics/a-day-in-data
[69] https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf
[70] https://healthitanalytics.com/news/big-data-to-see-explosive-growth-challenging-healthcare-organizations

The health system overall can be significantly improved when these medical data are shared among health stakeholders, data producers (e.g. hospitals, primary healthcare centres, health clinics, clinical analysis laboratories), citizens (as health data providers), and data consumers (e.g. research institutions, health authorities, pharmaceutical industry, drug agencies, insurance companies). Such sharing is possible through a data exchange market platform that shares data between different stakeholders. The data exchange platform provides data consumers access to data shared by the data providers.

Conversely, a lack of data sharing has a negative impact on the development of computer-based solutions. This negative impact affects areas such as imaging-based machine learning technologies which (i) are able to simulate surgical treatments or device implants, (ii) are able to automatically detect pathological lesions and (iii) are able to cross-reference imaging findings with other patient data for highly personalized clinical predictions. The data required for developing and testing these systems exists today in large quantities inside hospital firewalls[71,72,73], but it cannot be accessed without jeopardizing patient privacy and exposing institutions to severe legal implications.

The GDPR has established a much-needed legal framework that sets clear boundaries for compliant data exchanges and provides clear guidance to economic players, finally framing biomedical data sharing within legal boundaries and opening the possibility for trading such data under different classifications and corresponding legal agreements. The issue still to be solved is the need for a robust and scalable solution to enforce privacy and security requirements in a way that efficiently meets the strong demand for health data.

The medical data exchange demonstrator, leveraging an existing data exchange marketplace (Dawex[74]), 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.

---

[71] Raman SR et al. Leveraging electronic health records for clinical research. Am Heart J. 2018 Aug;202:13-19. 2018.04.015. 2018

[72] Yim W. et al Secondary use of electronic medical records for clinical research: challenges and opportunities, Conv. Science Physical Oncology, vol. 4,1, 2018

[73] http://www.appliedclinicaltrialsonline.com/how-ehrs-facilitate-clinical-research

[74] 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**[75].

8.3.2 What is expected to go wrong?

In a sector such as health data exchange, where sensitive data is managed, all the players/stakeholders involved must be aware of the risks when managing this kind of data. For this reason, the use and development of security and privacy tools, compliance with regulations and observance of standardized procedures are essential for preventing things from going wrong. Because of the significance of this kind of data, the health care sector in general has become a clear target for cybersecurity attacks.

Healthcare data breaches reported in the USA have increased sharply in recent years (2009-2018), from 18 cases during 2009 to one case per day during 2018[76]. According to the 2019 Data Brach Investigations Report performed by Verizon[77], which included data from 86 countries around the world, 466 incidents were reported, of which 304 declared data disclosure.

Intentional hacking, IT incidents, unauthorized data access/disclosure, theft, loss and even inadequate disposal are the main threats. Additionally, ECSO in the Healthcare Sector Report points out that the "use of cloud services, unsecure networks, employee negligence, bring your own device (BYOD) policies, lack of internal identification and security systems, stolen devices with un-encrypted files and others[78]", are potential causes of data breaches. Unfortunately, the leading causes of breaches that occurred this year in the UK were related to human error (incorrect disclosure to wrong recipient or replying to a phishing attack), followed by wrong data shown, loss, theft or even direct communication of personal data[79]. 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.

---

[75] https://www.researchgate.net/publication/234034137_Protecting_Patient_Privacy_when_Sharing_Medical_Data
[76] https://www.hipaajournal.com/healthcare-data-breach-statistics/
[77] https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief-emea.pdf
[78] https://www.ecs-org.eu/documents/publications/5ad7266dc1cba.pdf
[79] https://www.healthcareitnews.com/news/europe/statistics-reveal-healthcare-sector-most-affected-personal-data-breaches

8.3.3 What is the worst thing that can happen?

In the medical data exchange scenario, the main kind of impacts are related to the following aspects:

- User privacy;
- Integrity of the data;
- Data breach;
- GDPR compliance.

Considering these aspects, the worst-case scenarios are as follows:

- Sensitive data and health records can be stolen by intruders if the security mechanisms fail.
- Recurrent data breaches will occur if the system is not secure enough or the control and tracking of activities on the platform are not well monitored and checked appropriately.
- Users' private data may be lost if data is exposed to the public. The loss of sensitive data belonging to citizens and patients will mainly cause privacy issues. Depending on the final recipient of this data, the user's normal life can be affected in different ways. If these sensitive records (health records, genetic information) reach insurance companies, they could leverage this information to justify increasing premiums, charging extra payments or even rejecting users who have health problems.
- Public health IT infrastructure may suffer crashes if software or hardware vulnerabilities are exploited by malicious third parties.
- Loss of life may occur when IT health infrastructures are endangered and the integrity of the data is compromised, if data is lost or not available to health personnel (doctors, nurses, care assistants, etc.) on emergency cases.
- Trust and confidence from users, data providers and data consumers may be compromised if data sharing platforms manage the stored data in an inappropriate manner.
- Considerable fines may be imposed if a data sharing platform fails to comply with the applicable regulations, such as GDPR.
- Financial losses may be caused by one of more of the above scenarios. According to the GDPR regulations, data breaches are penalized by EU Member State authorities[80], 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:

- **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;
- **Hacktivists,** acting for political reasons or against the practices of some pharmaceutical companies;

[80] https://gdpr.eu/fines/

- **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;
- **Insider,** 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 health data is managed by private companies. Recently Project Nightingale[81] has been involved in a "secret transfer of medical history data, which can be accessed by Google staff"[82]. Apparently, health data has been delivered, including personal data. Therefore, not only must security measures be put in place to prevent attacks from external attackers, but measures must also be taken to avoid personal and sensitive data being made public by internal staff.

As indicated before cybersecurity practices must be followed to manage threats and preserve personal and sensitive data[83].

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 regulation[84] 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 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

[81] https://www.theatlantic.com/technology/archive/2019/11/google-project-nightingale-all-your-health-data/601999/
[82] https://www.theguardian.com/technology/2019/nov/12/google-medical-data-project-nightingale-secret-transfer-us-health-information
[83] https://tinyurl.com/r37vb7o
[84] https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

accessing data and innovative mechanisms for transaction tracking (e.g. blockchain) must be implemented.

- ***Provide tools for securing data in transit.*** Secure data exchange solutions must be built when sensitive data are transferred from the data producers to the data consumers, the security during the transference process must be assured.
- ***Updating data exchange platforms.*** On data sharing platform infrastructures, hardware and software updates must be applied regularly to avoid vulnerabilities that could be exploited by different attacks (e.g. data breaches, hacking, bugs, etc.).
- ***Keep the integrity of the data.*** Data loss or issues related to the integrity of the data can affect adequate patient evaluation and the procedures used to treat the patients. In this context, data integrity is needed during the course of a health treatment and the data must be managed in a privacy-preserving way by the data consumers (e.g. research institutions).

JRC Cybersecurity Domain:

- Data security and privacy
    - Design, implementation, and operation of data management systems that include security and privacy functions
    - Unlinkability
    - Data usage control
- Identity and access management (IAM)
    - Identity management models, frameworks, services (e.g. identity federations)
    - Authentication/Access control technologies (X509 certificates, RFIDs, biometrics, PKI smart cards, SRAM PUF, etc.);
    - Protocols and frameworks for IAM
    - Identity management quality assurance
    - electronic IDentification, Authentication and trust Services (eIDAS)
    - Optical and electronic document security
- Software and Hardware Security Engineering
    - Security requirements engineering with emphasis on identity, privacy, accountability, and trust

JRC Sectorial Dimensions:

- Health

JRC Technologies and Use Cases Dimensions:

- Big data

8.5.2 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

8.5.3 Challenge 3: Trustworthiness on the data exchange platform

Security and privacy challenges are close linked with the **trust** challenges. A lack of security and privacy on data sharing platforms will affect directly the user's trust in this kind of platforms and is likely to decrease the willingness of citizens and patients to share health data. In this context, some controversies[85] 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

[85] https://www.thelancet.com/journals/landig/article/PIIS2589-7500(19)30163-3/fulltext

JRC Technologies and Use Cases Dimensions:

- Big data

8.5.4 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 (GDPR), 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 of health-related data, genetic data and biometric data unless the data subject has given explicit consent, or when processing is necessary either for purposes of preventive or occupational medicine, or for reasons of public interest in the area of public health. One needs to study how the medical data sharing is affected by the GDPR.
- ***Implement mechanisms for fulfilling the GDPR regulation.*** Under the GDPR both the data controller and processor must implement appropriate technical and organizational measures (as will be described in deliverable 4.2 Legal Framework, in progress to be submitted in M12) to ensure a level of security appropriate to the risk. Management of risk also brings into consideration the Data Protection Impact Assessment (DPIA). DPIA is essentially a legally required (for certain situations) but more limited form of risk management. When processing health data, especially on a large scale, the DPIA is basically mandatory[86]. Failure to carry it out a 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

[86] 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.

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

JRC Cybersecurity Domain:

- Legal aspects

JRC Sectorial Dimensions:

- Health

JRC Technologies and Use Cases Dimensions:

- Big data

8.5.5 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 CyberSec4Europeproject.

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 CyberSec4Europeproject.

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 FENTEC[87] 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.

8.7.3 Challenge 3: Trust mechanisms

As indicated in section 8.5.3, the user willingness to share sensitive data in a DEP is based on trust. For DEPs the trustworthiness is based on the implemented security mechanisms and the privacy-preserving measures the DEP applies on user data. In this context the described assets in sections 8.7.1 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.

[87] http://fentec.eu/

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 (Looker[88] and Board[89]) have been deeply analysed and carefully tested. Both products were tested by the team using real data in sandbox environments.

Table 6: 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)	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

[88] https://looker.com/learn/recorded-demo
[89] https://www.board.com/en

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

Considering the **research challenges** described in section 8.5, the plan during the next 12 months includes following activities:

- ***Starting the integration of eIDAS network using the SPeIDI asset* (*addressing the security and trust challenge*** described in sections 8.5.1 and 8.7.1). With this aim, appropriate protocols for accessing the French eIDAS node will be developed. Contacts will be made with French organizations managing the country's eIDAS node in order to proceed with testing activities.
- Additionally, the ***anonymization service (DANS) for addressing the security and privacy challenge*** in sections 8.5.2 and 8.7.2 ***will be developed*** and then offered by the medical data sharing platform.
- Further, in connection with the user experience challenge (section 8.5.5 and section 8.7.5) a ***visualization tool designed by Dawex will be developed***.

8.8.2 3-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*** *challenge included in sections 8.5.1, 8.5.2, 8.5.3, 8.7.1, 8.7.2, and 8.7.3:*

- ***Finalize the eIDAS network integration*** with the French eIDAS node and with the Dawex platform.
- Perform ***the integration of the crypto service for assuring end-to-end encryption***.
- ***Set the basis for the adoption*** (depending on the availability of assets) ***of SSI for decentralized access to the platform***.
- ***Provide guidelines describing how to use the services offered to data providers and data consumers by the exchange platform***, which could be extended to other data exchange domains.

Related with the ***regulation challenge*** *included in sections 8.5.4 and 8.7.4:*

- In order to produce the ***GDPR*** guidelines the regulation, best practices and opinions provided by the European Commission and different supervisory authorities will be reviewed to create a ***comprehensive guideline, usable for as many situations and circumstance as possible***.
- Additionally, ***research on Regulation matters and related tools will seek out ways for easier and better compliance with regulations such as GDPR and eIDAS***.
- ***An analysis of interoperability and cross-border compliance of the eIDAS compliant electronic identification, security, and authentication services*** will be performed to identify flaws and compatibility of solutions between member states.

8.8.3 Beyond the end of the project plan

As part of the future work after the end of the project, some activities that can be developed for improving the medical data exchange platform are indicated here.

- Dawex will provide a ***hybrid data exchange platform, with blockchain capabilities and functionalities for the identity management***, (that will 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 the 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***.

9 Smart Cities

9.1 The Big Picture

Today, an increasing number of people worldwide live and work in cities. Consequently, creating livable environments in which people and businesses can thrive has become one of today's most pressing issues: the way we all use the time and the space available, the environment and the resources at our disposal determines the quality of our life and forms the basis for the sustainability of our existence in the medium and long term[90] . For that reason many cities and metropolitan areas are embracing the "Smart City" concept, that is adopting a more efficient management of services and turning cities into enablers of innovation, economic growth, and well-being, but also safe, dynamic and inclusive.

This transformation process needs all levels of government together with organizations and networks of cities and communities of all sizes, with strong cooperation through multi-level governance and co-creation with citizens. To do this, a first step is needed: the smart city (SC) enablers' adoption. The role of these enablers is to connect consumers and producers, enabling a federated publication of context data, allowing service providers to find and use data from city and third-party sources while preserving data sovereignty[91].

Digital solutions underpinned by locally-generated data are essential for delivering more informed, innovative and high-quality services to the public and to businesses. These solutions include smart urban mobility, energy efficiency, sustainable housing, digital public services and civic-led governance. If the public is to trust these systems, data must be used responsibly through digital platforms, and its quality, security and privacy must be ensured[92].

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

---

[90] https://www.eng.it/resources/whitepaper/doc/augmented-city/augmented-city-whitepaper-eng_.pdf

[91] https://www.fiware.org/community/smart-cities/

[92] https://www.living-in.eu/declaration

- Resource Providers - universities, urban planners, think tanks, and technical companies
- Framework Enablers - City councils, elected officials, standardization committees, and financial organizations

We can sketch a smart-city value chain with the following picture, to explain relations and dependencies between the stakeholders and the services:

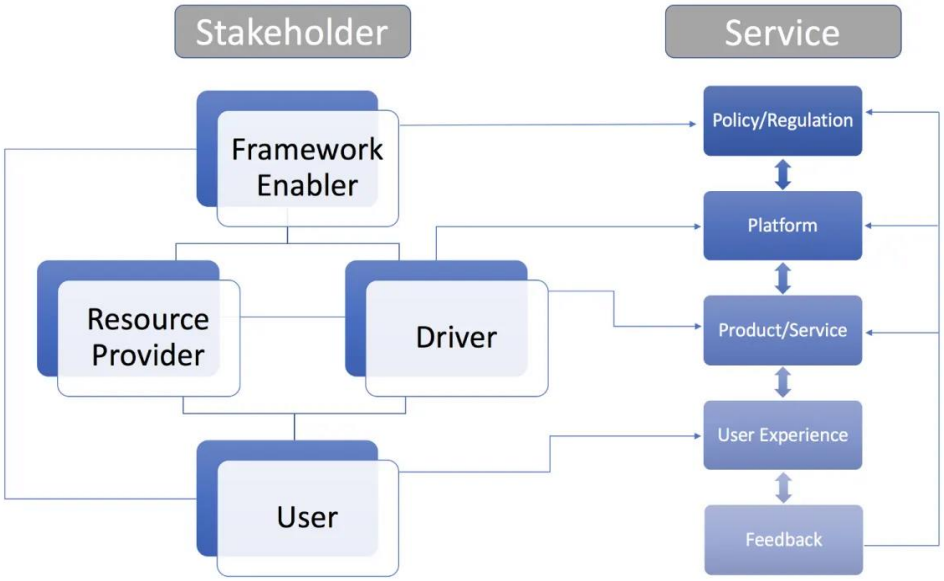


Figure 9: Stakeholders and the services

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. An SC 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.

Of course, this is not an immediate process, an LPA must first equip itself with the necessary tools. The enabling architecture for introducing the IoT in the cities has 4 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 the answers to a few questions, in order to give a clear context of the SC domain. A list of these research challenges may 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 an SC: these 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 an 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.

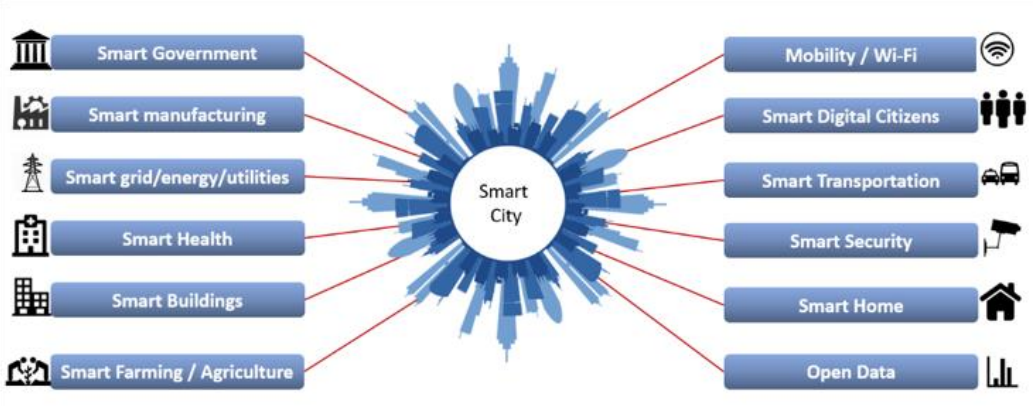


Figure 10: SC Stakeholders (Source: [CER 2019])

ENISA provides several white papers about **good practices for IoT and smart infrastructure tools**[93], 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.

[93]https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool/results#IoT

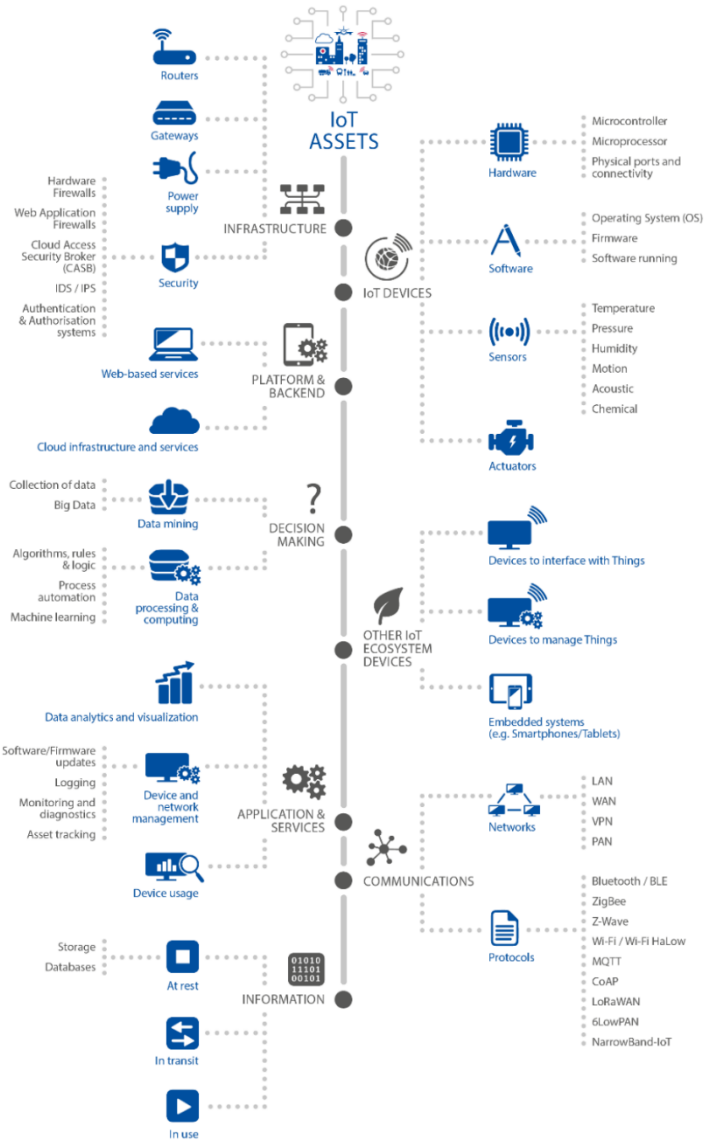


Figure 11: IoT Assembly Taxonomy (Source [ENISA 2018]).

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 take place more and more in the digital realm, creating a shear force between the availability of data and confidentiality that will be difficult to overcome.

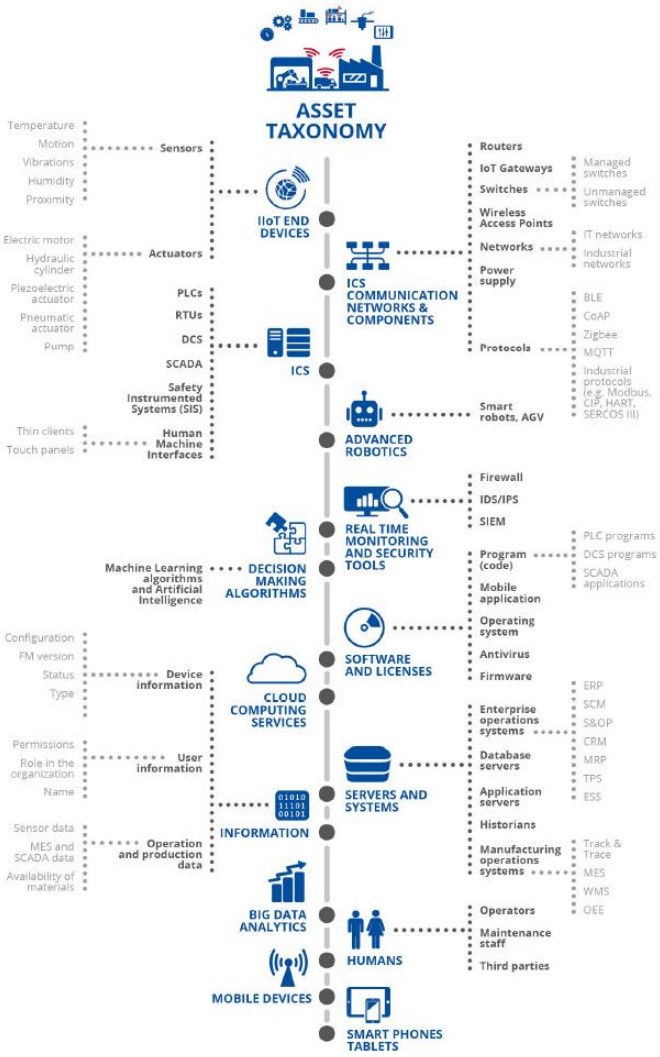


Figure 12: Industry 4.0 Asset Taxonomy (Source: [ENISA 2018]).

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 13 illustrates the threat taxonomy identified by ENISA. Most of the potential threats are basically related to **privacy, data & identity theft, device hijacking, denial of service, application level distributed denial of service, and man-in-the-middle attacks and ransomware.**

Man-in-the-middle[94]: 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.

[94] https://capec.mitre.org/data/definitions/94.html

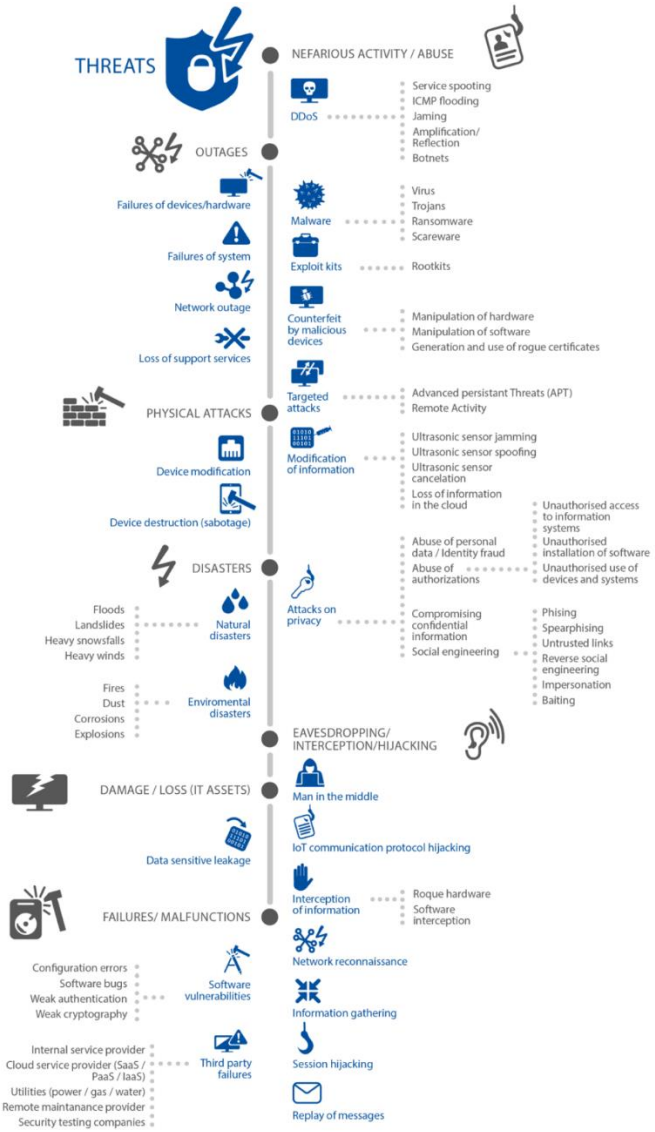


Figure 13: IoT Threat Taxonomy (Source: [ENISA 2018])

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 13 , Figure 14 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.** In the case of, for instance, 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 may be singled out from among the many and are described below:

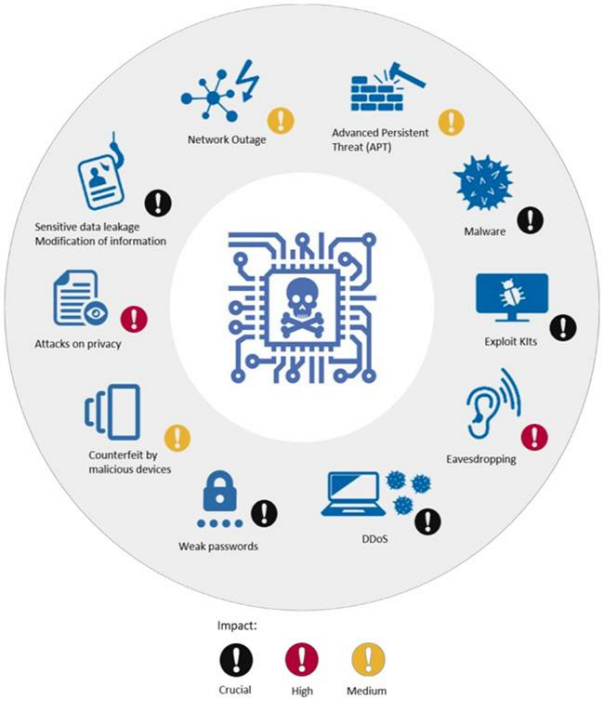


Figure 14: IoT Threats Impact

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.[95] 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.[96]

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, 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.

---

[95] https://www.theregister.co.uk/2016/04/12/sweden_suspects_russian_hackers_hit_air_traffic_control/
[96] https://www.scmagazineuk.com/ddos-attacks-delay-trains-halt-transportation-services-sweden/article/1473963

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 15 lists the threat agents according to the **Intel Threat Agent Library** [Intel 2007]. 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
Hostile	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
	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 15: Intel Threats Agents Identification

9.5 Research Challenges

9.5.1 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, 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 considered during platform realization so as to assure the management of heterogeneous network and communication, integration of different systems and components, the adoption of IaaS, SaaS and hybrid cloud environments.

JRC Cybersecurity Domains:

- Data Security and Privacy
  - Design, implementation, and operation of data management systems that include security and privacy functions;
  - Anonymity, pseudonymity, unlinkability, undetectability, or unobservability;
  - Privacy Enhancing Technologies (PET);
  - Digital Rights Management (DRM);
- Identity Management
  - Protocols and frameworks for authentication, authorization, and rights management;
  - Privacy and identity management (e.g. privacy-preserving authentication);
- Incident Handling and Digital Forensics
- Network and Distributed Systems
  - Network security (principles, methods, protocols, algorithms and technologies);
  - Distributed Systems Security;
  - Managerial, procedural and technical aspects of network security;
  - Network layer attacks and mitigation techniques;
  - Secure distributed computations;
- Software and Hardware Security Engineering
  - Security and risk analysis of components compositions
  - Secure software architectures and design;
  - Security design patterns
  - Self-including self-healing, self-protecting, self-configuration systems; Self-healing systems
- Trust Management and Accountability

JRC Sectorial Dimensions:

- Energy
- Defence
- Safety and Security
- Transportation

JRC Technologies and Use Cases Dimensions:

- Information Systems
- Critical Infrastructures
- Hardware technology
- Protection of public spaces
- Industrial IoT and Control Systems
- Internet of Things, embedded systems, pervasive

9.5.2 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;

9.5.3 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;

9.5.4 Challenge 4: Privacy by design

Privacy by design encompasses seven principles that should be followed [Cavoikian 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 re**gu**lation 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;
- Internet of Things, embedded systems, pervasive systems;
- Mobile Devices;
- Operating Systems;
- Vehicular Systems (e.g. autonomous vehicles);

9.5.5 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);

9.5.6 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 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 includes the management of secure channels.
- ***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.

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;
- Internet of Things, embedded systems, pervasive systems;
- Mobile Devices;
- Operating Systems;
- Vehicular Systems (e.g. autonomous vehicles);

9.5.7 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 application that should work in collaboration. Specific verification and validation approaches and means should considered so as to assure the interoperability between legacy and new systems.

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);

9.5.8 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 fulfill 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.

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.

JRC Cybersecurity Domains:

- Security Management and Governance
    - Risk management, including modeling, assessment, analysis and mitigations;

    - Threats and vulnerabilities modeling;
    - Attack modeling, 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
- 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);

9.5.9 Challenge 9: Logging and monitoring

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. 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 behavior 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.

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);

9.5.10 Challenge 10: Information security and operational security

Given the variety of services, systems and applications that share the servers and resources involved in SC, one growing threat is the encryption of files and data by ransomware. There is an urgent need to develop measures to protect against ransomware, and malware in general, that might compromise the critical infrastructure.

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.

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 platforms 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 an 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 behavior 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 7: 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	• **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	• **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	• **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	• **GENERAL_D** (D3.1, Section 5.1) • PPIdM (D3.1, Section 5.1)	The WP3 and WP5 tools cover 5 of the 7 seven “Privacy by Design”

		• **PLEAK** (D3.1, Section 5.2) • **CaPe** (D5.2, Section 8.2.3.2)	principles. The following ones need to be addressed beyond the project: • full functionality with full privacy protection; • privacy protection through the entire lifecycle of the data.
Challenge 5	Cyber response and resilience	• **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	• 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)	Auditing and accountability procedures
Challenge 7	Interoperability between legacy and new systems	• **SPeIDI** (D3.1, Section 5.1) • **PTASC** (D3.11, Section 5.8) • eIDASBrowser (D3.1, Section 5.1) • PPCTIs (new asset)	Legal Aspects Formal verification of security assurance Software and Hardware Security Engineering Theoretical Foundations
Challenge 8	Cyber fault/failure detection and prevention	• **Briareos** (D3.1, Section 5.3) • **RATING** (D5.2, Section 8.2.3.2)	Theoretical Foundations
Challenge 9	Logging and monitoring	• **CaPe** (D5.2, Section 8.2.3.2)	Auditing and accountability procedures
Challenge 10	Information security and operational security	• **Mobile p-ABC** (D3.1, Section 5.1) • PPCTIs (new asset) • 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 COMPACT[97] 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.
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 16) 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.

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

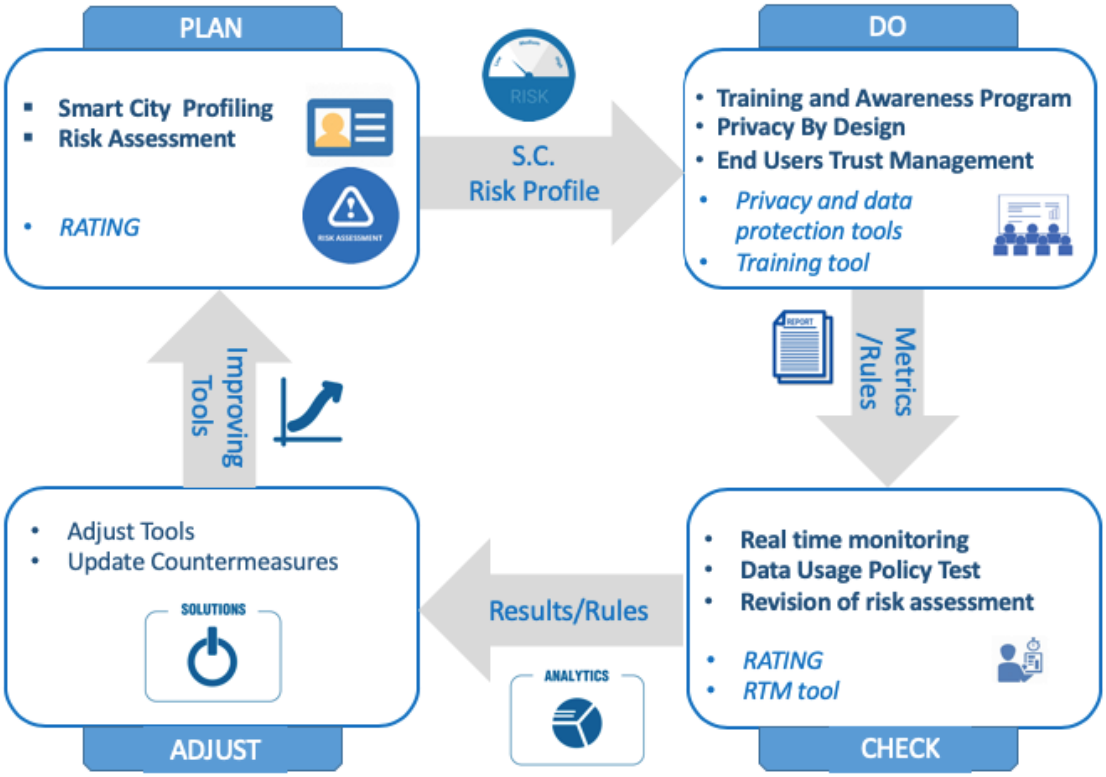


Figure 16: PDCA cycles for SC vertical

With the increase in integration between digital and physical worlds, SC need to identify and evaluate emerging risks and, especially, evaluate the cascading effects of a potential attack.

Nowadays, there are several methods and frameworks; among these, the NIST cyber security framework provides best-practices and guidelines for improving the cybersecurity of critical infrastructure[98] (in line with ISO31000).

Following the NIST directive, risk assessment is part of the identification stage, whose aim is to establish the context, profile the infrastructure, identify assets and businesses to protect, evaluate impacts and highlight emerging risks associated with the infrastructure's vulnerabilities.

Regarding security measures for the protection of personal data, following a risk-based approach, ENISA has also provided guidelines[99] 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, and evolving, existing tools, and will include:

[98] https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf
[99] https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

- 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.

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 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 (GDPR) – 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 2.2 and the identified methodologies and tools, the following research roadmap is defined.

9.8.1 12-month plan

This phase aims to generate a common understanding among all the involved partners and to prepare end-users to perform the relevant activities in terms of internal commitment and organization.

Risk assessment. The next 12 months will be focused primarily on context establishment. More specifically, activities are limited to the early identification of the stakeholders' protection goals, their data operation processes and foreseen impacts, in order to provide an early identification of possible risk scenarios and their analysis in relation to possible cascading effects.

Trusted Digital Platform. We plan to evaluate the integration of some Trusted Digital Platform tools provided by the partners' consortium. Special attention will be directed to authentication, user transparency and data protection.

Privacy by design. In the next 12 months of the project, the already identified tools for risk assessment, solution elicitation and consent-based personal data management will be put into operation in the identified use case. In addition, we are working on the identification 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.

Cyber threat intelligence and analysis platform. In order to obtain detailed risk profiles for stakeholders, we plan to evaluate the integration of some cyber threat intelligence tools provided by the partners' consortium. Particular attention will be directed to the identification and classification of cyber threats in order to provide useful datasets.

Cyber response and resilience. We plan to work on developing methodologies and tools to improve the cyber response and resilience so as to be prepared for potential social engineering attacks. This also includes:

- understanding the digital shadow of the stakeholder experience with OSINT research strategies;
- developing attack simulation scenarios.

Cyber competence and awareness program. We plan to work on developing gamification methodologies and tools to improve cyber competences and cyber-related capabilities for human aspects. More specifically, early identification of the most relevant cyber competence leaks will be sought (through surveys, face-to-

face meetings, etc.) in order to design and develop game-based cyber security awareness programs to be implemented in the mid-to-long term.

9.8.2 3-year (or until the end of the project) plan

Risk assessment. Based on the results of the previous 12 months, we will plan, execute and analyse risk assessment instances by setting-up an open innovation cycle that will drive city stakeholders from cybersecurity risks and needs assessment to the identification of the related solutions (i.e. cybersecurity services) as well as cybersecurity risk assessment tools and social engineering penetration testing tools.

Privacy by design. For the SC demonstration case, we will focus on setting up and putting into operation a consent-based infrastructure to support sensor and other urban data platforms, and an infrastructure for personal data exchange and reuse in public services, in compliance with GDPR.

Cyber response and resilience. We plan to put in place a social-driven vulnerability assessment that enables city stakeholders to face the risks related to human cybersecurity capabilities. This also includes:

- the provision of anonymized data to risk assessment modules;
- an analysis of both human and technological vulnerabilities.

Cyber competence and awareness program. We plan to put in place and improve several awareness methods designed in the previous phase.

9.8.3 Beyond the end of the project plan

It is obviously complex 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 are taken over by the software houses, which will have the task of customizing and spreading 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 successfully cases like London, Amsterdam and Paris, and the small Reykjavík [IESE 2019], demonstrate that a real change can be made in people's minds.
- **Adapt governance structures**: this aspect could be affected by the typical resistance to changing of Public Administration due to the bureaucratic process needed to perform any governance innovation. For this reason, it is more realistic to think that it will be a long process.

10 Common Challenges

Recently, the European Commission's Joint Research Centre published a taxonomy of cybersecurity research areas[100]. To see how the research challenges of Cybersec4Europe map onto the JRC research areas, as viewed not only by the members of each vertical, but by the members of all verticals, we created a questionnaire[101] and invited the WP4 partners to fill it in and say which JRC research areas are important for their vertical.

The research areas identified by the JRC are:

- Assurance, Audit and Certification
- Cryptology (Cryptography and Cryptanalysis)
- Data Security and Privacy
- Education and Training
- Human Aspects
- Identity Management
- Incident Handling and Digital Forensics
- Legal Aspects
- Network and Distributed Systems
- Security Management and Governance
- Security Measurements
- Software and Hardware Security Engineering
- Steganography, Steganalysis and Watermarking
- Theoretical Foundations
- Trust Management and Accountability

A common problem encountered in such questionnaires when asking people "Which research areas are important for your area?", would be to receive an answer in the form: "all of them". To "force" them to prioritize and really choose the most important areas we limited the answers to at most three areas. That is, each participant could select no more than three areas.

[100] https://ec.europa.eu/jrc/en/publication/proposal-european-cybersecurity-taxonomy
[101] https://ec.europa.eu/eusurvey/runner/CyberSecurityForEuropeWP4 .

10.1 Open Banking

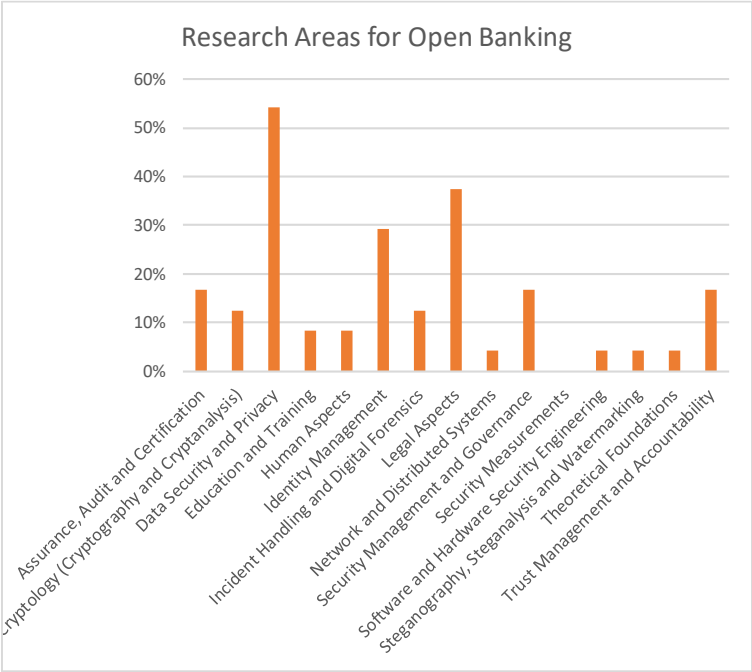


Figure 17: Research Areas for Open Banking

Figure 17 shows the Research areas that are important for the vertical of Open Banking. We see that the areas of Data Security and Privacy, Legal Aspects, and Identity Management rise above the rest. This is not unexpected. Indeed, without strong privacy, open banking (or any form of online banking) will not be able to gain people's trust. Similarly, since we are talking about open banking (i.e. opening the data to "eyes" beyond those of the bank), strong identity management and strong authentication are of significant importance here. It is interesting to see that Legal Aspects have also risen above the rest. Indeed, without appropriate legal and regulatory support, technical solutions in this area will probably not be enough. Interestingly, section 3.5 is in line with the JRC priorities identified.

	Data Security and Privacy	**Legal Aspects**	**Identity Management**
Research challenges proposed in section 3	Stakeholder Interaction Setting up Business Relationships Cross Border Cooperation	Cross Border Cooperation	Convenient and Compliant Authentication Real-time revocation of Access Rights

10.2 Supply Chain Security Assurance

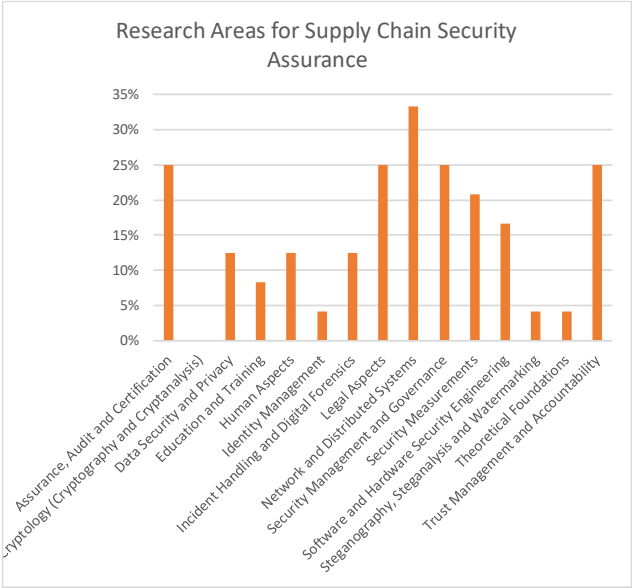


Figure 18: Research Areas for Supply Chain Security Assurance

Figure 18 shows the research areas considered important in the Supply Chain vertical. As before, we see that most cybersecurity research areas are present. However, two or three stand out, including Network and Distributed Systems, Legal Aspects, Security Management and Governance, as well as Assurance, Audit and Certification, and finally, Trust Management and Accountability. For example, since the supply chain is by definition geographically distributed, research in Network and Distributed Systems is paramount. Similarly, since the supply chain may cross several national boundaries and jurisdictions, Legal Aspects have a key role. Once again, since this is a traditional business area, risk management and mitigation (all included in Security Management and Governance) are also very important.

	Network and Distributed Systems	Legal Aspects	Security Management and Governance	Assurance, Audit, and Certification	Trust Management and Accountability
Research challenges proposed in section 4	Security hardening of supply chain infrastructures		Detection and Management of Supply Chain security risks	Management of the accreditation of supply partners	Security and Privacy of supply chain information assets and goods

10.3 Privacy-preserving Identity Management

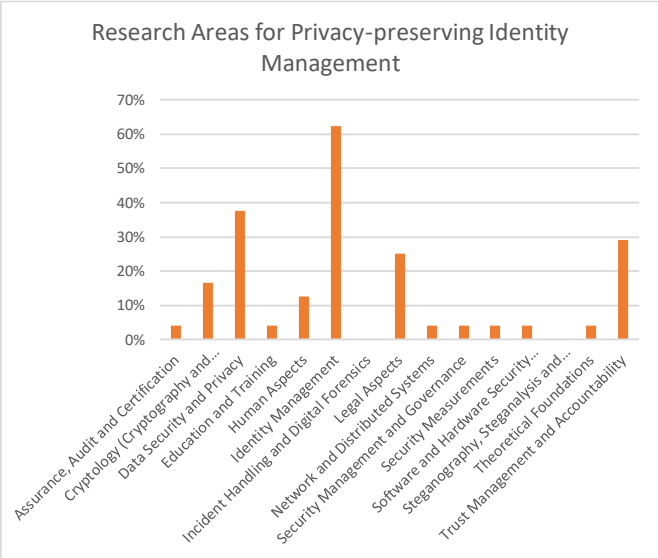


Figure 19: Research Areas for Privacy-preserving Identity Management

In the area of "privacy-preserving identity management" (Figure 19) we see that, unsurprisingly, "Identity Management" comes first. "Data Security and Privacy" also looks very important, and last, but not least, "Trust Management and Accountability" is among the top three cybersecurity research priorities.

	Identity Management	Data Security and Privacy	Trust Management and Accountability
Research challenges proposed in section 5	System-based credential hardenings Distributed oblivious Identity Management Passwordless authentication	Unlinkability and minimal disclosure	Privacy preservation in blockchain

10.4 Incident Reporting

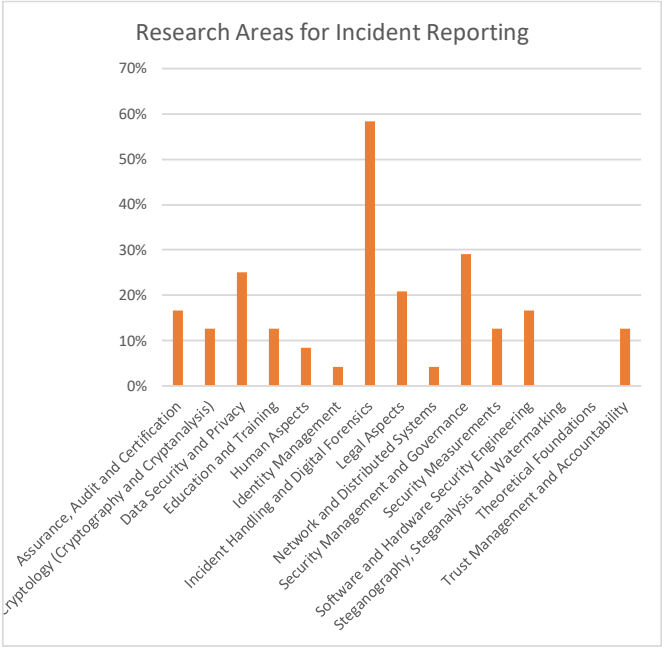


Figure 20: Research Areas for Incident Reporting

The vertical of "Incident Reporting" is clearly different from the rest. Indeed, although the rest of the verticals have to deal with cyberattacks, this vertical is not necessarily under constant attack from cyberattackers. Despite that, there is still research that needs to be done in this area. Obviously, as we can see from Figure 20, the top area is "Incident Handling and Digital Forensics", which should come as no surprise for a vertical called "Incident Reporting". The next two most important areas are "Data Security and Privacy" (as incidents may result in data loss and may need data sharing) and "Security Management and Governance" (since Incident Reporting is a part of Security Management).

	Incident Handling and Digital Forensics	Data Security and Privacy	Security Management and Governance
Research challenges proposed in section 6	Incident Data Collection Incident Impact Assessment Incident Reporting	Threat Intelligence information systems and services	Incident Impact Assessment

10.5 Maritime Transport

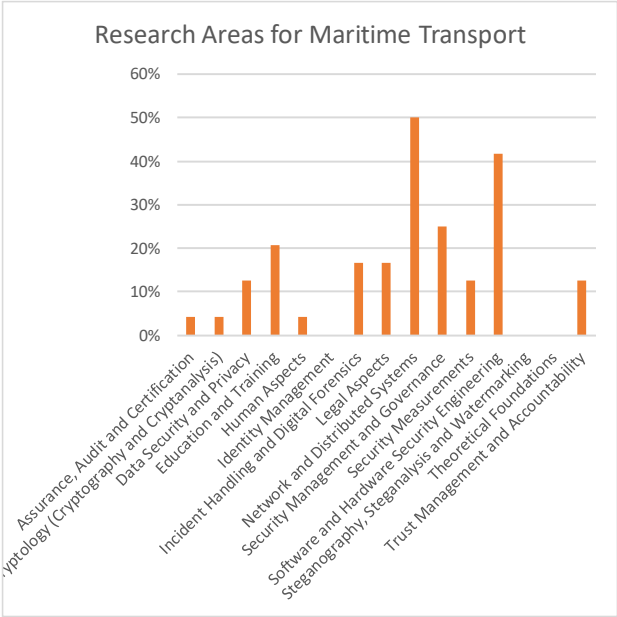


Figure 21: Research Areas for Maritime Transport

In the vertical of Maritime Transport (see Figure 21), the horizon is clear: "Network and Distributed Systems" along with "Software and Hardware Engineering" appears at the top the list. This should come as no surprise, as Maritime involves a collaboration between a network of distributed systems. Such systems may run vulnerable software (and possibly hardware) whose security should be improved. A third area that can be seen as well is "Security Management and Governance" which includes "Risk Management" - a practice used in Maritime for several years now – even before the introduction of computers.

	Network and Distributed Systems	Software and Hardware Hardening	Security Management and Governance
Research challenges proposed in section 7	Maritime system communication security Securing autonomous ships Resilience of critical maritime systems	Security hardening of infrastructures	Early Identification and Assessment of Risks

10.6 Medical Data Exchange

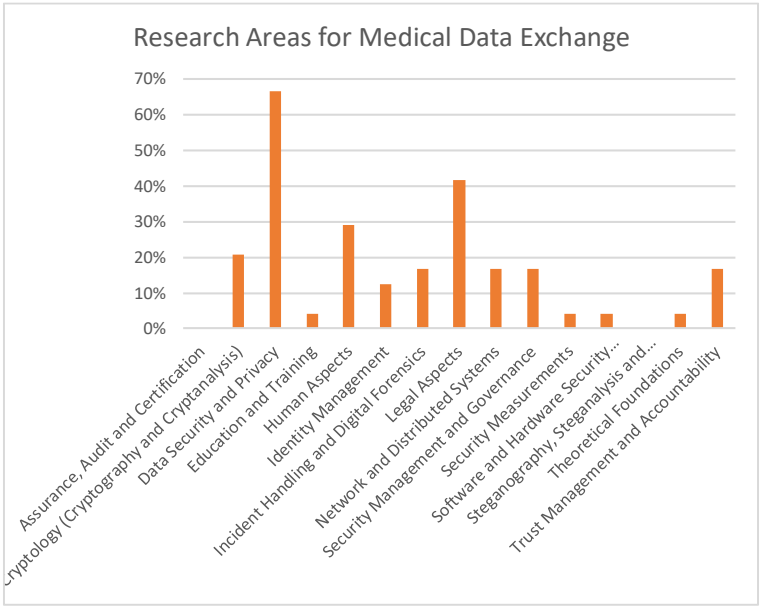


Figure 22: Research Areas for Medical Data Exchange

Figure 22 shows the important research areas for the "Medical Data Exchange" vertical. The clear winner here is "Data Security and Privacy". This should come as no surprise. Medical data is very sensitive data where a possible leak may have devastating consequences for people and their families. Making sure that they are protected is of paramount importance. Following close behind are "Legal Aspects" and "Human Aspects" which are both very important when dealing with sensitive personal data such as medical data.

	Data Security and Privacy	Legal Aspects	Human Aspects
Research challenges proposed in section 8	Security and Privacy Trust	Regulation	User Experience

10.7 Smart Cities

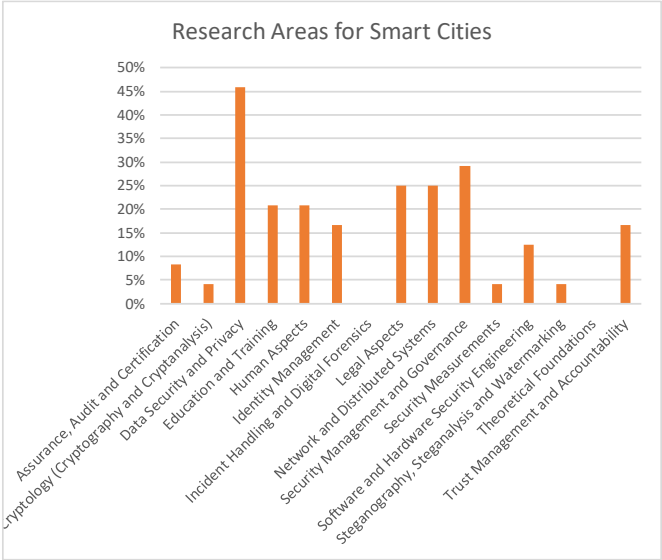


Figure 23: Research Areas for Smart Cities

In our last of the verticals which deals with "Smart Cities" Figure 23 shows that that "Data Security and Privacy" appears to be the clear winner. Indeed, Smart Cities will collect lots of data from all kinds of sensors. Ensuring the Security and Privacy is the most significant concern. "Network and Distributed Systems", "Legal Aspects", and "Security Management and Governance" follow next, and this is not surprising as all these are very important when dealing with collecting (potentially) personal data in a possibly unfriendly environment outdoors.

	Data Security and Privacy	Legal Aspects	Security Management and Governance	Network and Distributed Systems
Research challenges proposed in section 9	Privacy by Design Trusted Digital Platform		Risk Assessment Cyber Response	Cyber Threat Intelligence and analysis

10.8 All verticals

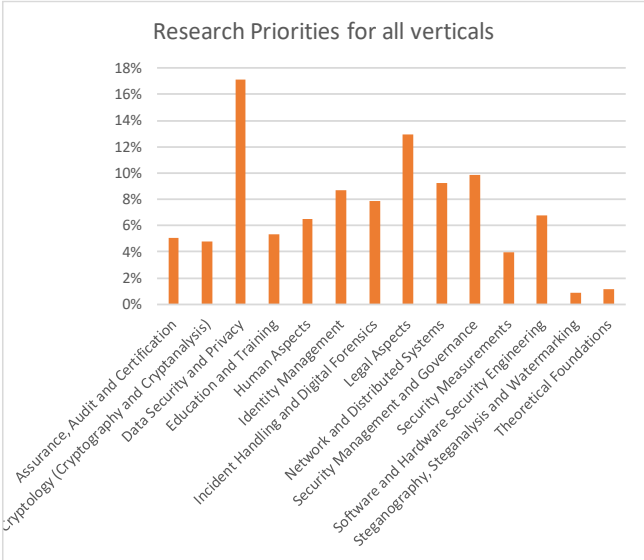


Figure 24: Research areas needed by the industrial challenges of CyberSec4Europe

Figure 24 shows which research areas are important overall. We see that "Data Security and Privacy" appears to top them all. Focusing on "Data Security and Privacy" we see that it includes the following topics [JRC 2019]:

- 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);
- Risk analysis and attacks with respect to de-anonymization or data re-identification (e.g. inference attack);
- Eavesdropping techniques (e.g. via electromagnetic radiation, visual observation of blinking LEDs, acoustic via keyboard typing noise);
- Data usage control.

Next, "Legal Aspects", "Security Management and Governance", and "Network and Distributed Systems" follow closely.

11 Summary

This document presents a CyberSecurity Roadmap for the seven verticals identified in the CyberSec4Europe project: (i) Open Banking, (ii) Supply Chain, (iii) Privacy-preserving Identity Management, (iv) Security Incident Reporting, (v) Maritime Cybersecurity, (vi) Medical Data Exchange, and (vii) Smart Cities.

To be able to present their research challenges in a uniform way, all verticals followed a common structure (to the extent possible) as shown below:

- *Introduction*
  - ***Big Picture**: What is the broad setting of the vertical?*
  - *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?*
- *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**?*

11.1 The attackers

Before identifying the research challenges themselves, we first identified the cyber attackers. This helped us understand not only **what** we need to protect, but **whom we need to protected it from**. The table below also shows who are the main attackers considered in the various verticals. We see that typical attackers include hackers, (business) competitors, insiders, mobsters, activists, governments, irrational people, and, last but not least, terrorists. We see that hackers, competitors, and insiders top the list. These groups of attackers have different interests and vastly different capabilities.

	Terrorists	Hackers	(Business) Competitors	Insiders	Mobster	Governments – Intelligence Services	Activists	Irrational people
Open Banking	X	X	X	X				
Supply Chain	X	X		X	X			
Privacy-preserving identity management		X	X	X				
Maritime Transport	X	X	X	X	X	X	X	X

Medical Data Exchange	X	X	X	X			X	
Smart Cities	X	X	X	X	X	X	X	X

11.2 The Research Challenges

Once we identified the attackers, we set out to identify the research challenges that we need to address in order to protect the verticals from the attackers. The most important challenges identified per vertical are:

- Open Banking:
  - Mapping of stakeholder interaction in end-to-end Open Banking processing
  - Setting up and discontinuing business relationships
  - Cross-border cooperation under differing legislation and security controls
  - Convenient and Compliant Authentication
  - Real-time revocation of right of access
  - Corporate Open Banking Security
- Supply Chain Security:
  - Detection and management of supply chain security risks
  - Security hardening of supply chain infrastructures, including cyber and physical systems
  - Security and privacy of supply chain information assets and goods
  - Management of the accreditation of supply partners
- Privacy-Preserving Identity Management
  - System-based credential hardening
  - Unlinkability and minimal disclosure
  - Distributed oblivious identity management
  - Privacy preservation in blockchain
  - Password-less authentication
- Incident Reporting:
  - Lack of harmonization of procedures
  - Facilitate the collection and reporting of incident and/or data leaks
  - Promote a collaborative approach for sharing incident reports to increase cyber resilience
- Maritime Transport:
  - Early identification and assessment of risks, threats and attack paths for critical maritime systems
  - Security hardening of maritime infrastructures including cyber and physical systems
  - Resilience of critical maritime systems
  - Maritime system communication security
  - Securing autonomous ships
- Medical Data Exchange
  - Security and privacy
  - Trust
  - Regulation
  - User Experience
- Smart Cities
  - Trusted Digital Platform
  - Cyber threat intelligence and analysis platform
  - Cyber competences and awareness program

- Privacy by Design
- Cyber response and resilience
- End user trusted data management
- Interoperability between legacy and new systems
- Cyber fault/failure detection and prevention
- Logging and monitoring
- Information Security and operational security

We see that different verticals need to face different challenges. Ranging from cyberthreat intelligence to security hardening, all the way to securing autonomous ships, we see that no matter what the challenge is, we are bound to experience some very interesting results over the next few years.

Annexes

Annex I Methodology

In this section we will provide more details on the methodology used for the development of this Roadmap. To the extent possible, we aimed to follow a uniform approach for structuring all vertical roadmaps. Namely, all roadmaps have been organized using the following items, which will be further explained in the next subsections:

- Introduction – Big Picture
- 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?
- Describe the Research Challenges of this area
- Methods, Mechanisms, and Tools
- Roadmap
    - 12-month plan
    - 3-year (or until the end of the project) plan
    - Beyond the end of the project plan

I.1 Introduction

For every vertical, this section must describe the area of the vertical. It describes the problem we are trying to solve. It also describes the "big picture" that the vertical may cover.

I.2 What is at Stake

I.2.1 What needs to be protected

For every vertical, this section must list the important services and assets (HW, SW, data, other) that are involved in this vertical and that need to be protected. -- (critical asset identification)

I.2.2 What is expected to go wrong?

For every vertical, this section must describe events and attacks that may have happened or are likely to happen, and what harm they may be expected to cause. Note that here we focus on what is expected to happen in the "average" case or "everyday" scenarios, and not on "doomsday" outcomes. Some of the categories into which such events can be classified are found in NIST Special Publication 800-30 [NIST 2012], and are summarized here:

- **Perform reconnaissance and gather information**: This category of threat events entails scanning a target in order to acquire information about its attack surface. Performing this step allows the attacker to identify critical assets and services with a view to later attacking and possibly exploiting them.
- **Craft or create attack tools**: This category of threat events entails the invention of methods that will allow the initiation of contact with a target.
- **Deliver/insert/install malicious capabilities**: This category of threat events entails the ways in which malicious mechanisms can be planted in a target.

- **Exploit and compromise**: This category of threat events entails the exploiting of vulnerable or critical targets that were identified with the aid of installed mechanisms and attack tools.
- **Conduct an attack** (i.e. direct/coordinate attack tools or activities): This category of threat events entails a list of ways in which an adversary can perform an attack in order to harm the target and to enable further vulnerabilities, to be used as further opportunities for attacks
- **Achieve results**: This category of threat events is related to the effect an attack has on a target. (i.e. cause adverse impacts, obtain information)
- **Maintain a presence or set of capabilities**: This category of threat events entails techniques that aim to establish a strong presence in a target in order to discover further vulnerabilities and enable future attacks.
- **Coordinate a campaign**: This category of threat events entails the orchestration of meticulous plans that aim at the complete compromise of a target by planning and executing a vast chain of attacks.

More things expected to go wrong (even in the average case) can be found in section I.2.3 below.

I.2.3 What is the worst thing that can happen?

For every vertical this section must describe "worst case scenarios". These are "doomsday" scenarios or "what is the worst thing that can happen if everything goes wrong?". The goal of this section is to help us understand how severe an attack can be in the worst case. For example, a virus penetrating a computer that controls a nuclear power plant may have more devastating consequences compared to a virus penetrating a home thermostat. The worst-case scenarios for the two cases are very different. Possible things that can go wrong can also be found in NIST Special Publication 800-30 [NIST 2012], and are summarized here:

- **Harm to Operations**:
    - Inability to perform current missions/business functions:
        - In a sufficiently timely manner.
        - With sufficient confidence and/or correctness.
        - Within planned resource constraints.
    - Inability, or limited ability, to perform missions/business functions in the future.
        - Inability to restore missions/business functions.
        - In a sufficiently timely manner.
        - With sufficient confidence and/or correctness.
        - Within planned resource constraints.
    - Harms (e.g., financial costs, sanctions) due to noncompliance.
        - With applicable laws or regulations.
        - With contractual requirements or other requirements in other binding agreements (e.g., liability).
    - Direct financial costs.
    - Relational harms.
        - Damage to trust relationships.
        - Damage to image or reputation (and hence future or potential trust relationships).
- **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.

    - Damage to or loss of component parts or supplies.
    - Damage to or of loss of information assets.
    - Loss of intellectual property.
- **Harm to Individuals:**
    - Injury or loss of life.
    - Physical or psychological mistreatment.
    - Identity theft.
    - Loss of Personally Identifiable Information.
    - Damage to image or reputation.
- **Harm to other organizations:**
    - Harms (e.g., financial costs, sanctions) due to noncompliance.
        - With applicable laws or regulations.
        - With contractual requirements or other requirements in other binding agreements.
    - Direct financial costs.
    - Relational harms.
        - Damage to trust relationships.
        - Damage to reputation (and hence future or potential trust relationships).
- **Harm to the Nation**
    - Damage to or incapacitation of a critical infrastructure sector.
    - Loss of government's continuity of operations.
    - Relational harms:
        - Damage to trust relationships with other governments or with nongovernmental entities.
        - Damage to national reputation (and hence future or potential trust relationships)
        - Damage to current or future ability to achieve national objectives.
        - Harm to national security.

One may also potentially quantify the impact to these events, possibly as follows [NIST 2012]:

- **Very High:** The threat event could be expected to have multiple severe or catastrophic adverse effects on organizational operations, organizational assets, individuals, other organizations or the nation.
- **High**: The threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations or the nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and with a duration that prevent the organization performing one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals, involving loss of life or serious life-threatening injuries.
- **Moderate**: The threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations or the nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and with a duration that do not prevent the organization performing its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.

- **Low**: The threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations or the nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and with a duration that do not prevent the organization performing its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
- **Very Low**: The threat event could be expected to have a negligible adverse effect on organizational operations, organizational assets, individuals, other organizations or the nation.

I.3 Who are the attackers?

For every vertical, in this step we must identify the threat agents that pose significant danger to critical services [Casey 2007] [FIRST][NIST 2012].

Below we provide possible threat agent profiles (originally provided by Intel) adapted with enhanced descriptions according to the generic industrial requirements of the demonstration cases that will be further examined in the following sections.

- **Anarchists**: Individuals who reject all forms of structure, either private or public, and act within few, if any constraints.
- **Civil Activists**: Peaceful but highly driven individuals actively supporting a cause.
- **Competitors**: Contesting businesses that compete for revenues, resources and clientele.
- **Corrupt Government Officials**: Non-ethical individuals that take advantage of their position within the government in order to acquire resources.
- **Cyber Vandals**: Individuals who take amusement from penetrating and damaging existing assets. Cyber vandals do not present a strong agenda against specific targets.
- **Data Miners**: Professional data gatherers who acquire information through cyber methods without infiltrating an organization.
- **Disgruntled Employees**: Current or former employees who want to damage the company.
- **Government Spies**: 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.
- **Government Cyberwarriors**: Individuals who have significant resources at their disposal, which are state-sponsored and enable major disruption on a national scale.
- **Internal Spies**: Professional data gatherers as trusted insiders, generally with a simple profit motive.
- **Irrational Individuals**: Irrational individuals with absurd purposes.
- **Legal Adversaries**: Ill-willed individuals who take part in legal proceedings against the company, warranted or not.
- **Mobsters**: Individuals high in the command chain of organized crime who have significant resources available.
- **Radical Activists**: Individuals who are highly motivated to support a cause and are open to destructive methods.
- **Sensationalists**: Attention-grabbers who may employ any method for notoriety; looking for “15 minutes of fame”.

- **Terrorists**: Individuals who employ violent methods in order to support a personal socio-political agenda.
- **Thieves**: Individuals who employ an opportunistic mindset and usually act under simple profit motives.
- **Vendors**: Business partners who go after inside information in order to gain financial advantage over competitors in the field.

Depending on the situation one may find more types of attackers than those described above.

I.4 Describe the Research Challenges of this area

For every vertical, this section must outline what the specific Research Challenges are that must be solved in the short, medium and long term. We expect different verticals to have different challenges, although there could be some overlap. To the extent possible, these challenges could follow the terminology of the JRC taxonomy [JRC 2019].

I.5 Mapping of the Challenges in the Big Picture

How do the identified Research Challenges map in the big picture? Which aspects do they cover?

I.6 Methods, Mechanisms, and Tools

For every vertical, this section must explore the overlap of the Research Challenges with the methods, mechanisms and tools discussed in Work Package WP3. That is, (i) we write down methods and tools (or even algorithms) needed to meet the described research challenges, (ii) we identify which of those tools were (or are being) developed in WP3, and (iii) we determine which other additional tools/methods need to be developed.

I.7 Roadmap

For every vertical, the goal of this section is to separate the short-term research challenges from the longer-term ones. Hence, we must aim to classify the different challenges into three categories:

- 12-month: short term
- 36-month: before the end of the project
- Beyond the end of the project: important challenges that are too big (or too difficult) to be addressed within the project's duration.

I.7.1 12-month plan

Describes what research should be done in the next 12 months.

I.7.2 3-year (or until the end of the project) plan

Describes what is envisioned to happen until the end of the project.

I.7.3 Beyond the end of the project plan

Describes challenges that cannot be reasonably implemented within the lifetime of the project.

I.8 Placing the work in the context of the JRC Terminology

Although this methodology produces the research challenges which are needed for each vertical, it might be of limited use to people outside each vertical. Indeed, verticals may have their own terminology and their own vision that may not be clearly understood by people outside the area. To address this shortcoming, we collected the research requirements for each verticals in the terminology (two-level taxonomy) introduced by the European Commission's Joint Research Centre (JRC) [JRC 2019]. Indeed, JRC has created a taxonomy of research areas in cybersecurity [JRC 2019]. This is a very useful way to make sure (i) that different people use the same terminology, (ii) that different people use the same high-level topics for cybersecurity research, and (iii) that each high-level topic contains the same lower-level topics. To collect the information in the same way from all verticals we created a questionnaire: https://ec.europa.eu/eusurvey/runner/CyberSecurityForEuropeWP4

The questionnaire basically asks: Which of the following research topics identified by JRC are important for your vertical? JRC has identified 15 top-level research areas. Each top-level research area has several lower-level research areas, whose number ranges from four to twenty (depending on the top-level research area).

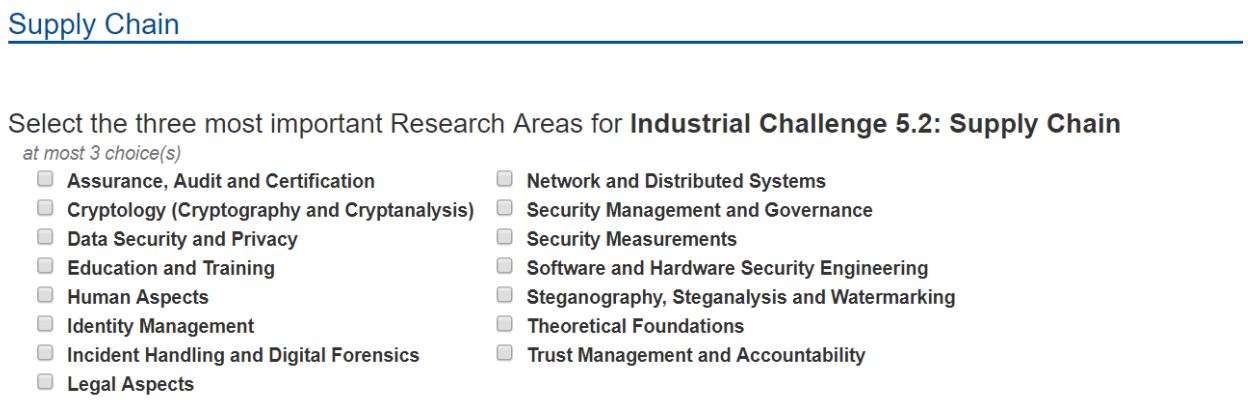


Figure 25: Sample Question taken from the Questionnaire on Research Priorities.

When constructing and distributing such questionnaires, one needs to be careful of the following caveat: when one asks people "which research areas are important", several people tend to answer "all/most of them". To avoid this obstacle and "force" people to prioritize, we did not ask them, "which are the important research areas", but we asked them to "select the three most important research areas". In this way, people have to select the three most important ones and thus prioritize among all the important research priorities.

We circulated the questionnaire to all WP4 participants in two phases: Firstly, we circulated the questionnaire among the WP4 participants who were present at the WP4 face-to-face meeting in Toulouse in November 2019. Secondly, we circulated the questionnaire via email to those WP4 partners who were not present at the WP4 meeting in Toulouse. We collected the results and for each vertical we identified the 3-4 most important research priorities according to the JRC terminology. The results can be found in section 10 on page 172.

Annex II Related Work

II.1 Cybersecurity: A Crisis of Prioritization

"Cyber Security: A Crisis of Prioritization" is considered one of the first and most important works [CYBER 2005] in this area. Ordered by the President of the United States, it came out immediately after the deployment of the large-scale worms, such as Code Red. The report accurately pointed out that the main line of defence is just "endless patching", which is just a race between attackers trying to find more exploitable bugs and software developers trying to patch as many software vulnerabilities as possible. The report proposed new research directions that would help bring an end to this vicious cycle. These directions included:

- Usable and reliable **authentication**
- Secure the **fundamental internet protocols**, such as BGP and DNS
- Secure **software engineering**
- **Holistic** System Security
- Security **monitoring** and detection of cyberattacks
- **Mitigation** of and recovery from cyberattacks
- **Cyber forensics**: catching criminals and deterring criminal activities
- Modelling and **testbeds** for new technologies
- **Metrics**, benchmarks, and best practices

II.2 FORWARD: Managing Threats in ICT Infrastructures

FORWARD was a pioneering project (Specific Support Action) that explored the emerging threats in ICT infrastructures. The main result of the project was a "White Book", which defined several research directions:

- "**Networking**. This area includes (i) attacks against the infrastructure of the Internet, such as against routers and routing algorithms; (ii) denial of service attacks, where strategic links or essential backbone nodes are taken out of service; and (iii) wire-tapping attacks, where the confidentiality or integrity of traffic is compromised on both wired and wireless links. In addition to attacks against the internet infrastructure, attacks may also be directed against end devices, including (i) denial of service attacks against servers on the internet, for example, by exploiting known vulnerabilities in applications or systems; (ii) distributed denial of service attacks, where the internet infrastructure and the large number of unprotected nodes on the internet are used to drown selected sites in traffic; and (iii) improper design or improper use of the services that the internet offers, for example, the design of mission-critical systems that are accessible from the internet and possibly in turn also depend on its services."
- "**Hardware and Virtualization**. This is probably the lowest level in the systems hierarchy where attackers may choose to operate. Although these attacks are usually difficult to deploy, they can remain stealthy for quite some time and thus be very effective. Such attacks may include (i) malicious hardware, and (ii) attacks within the cloud."
- "**Weak Devices**. Capitalizing on their small size and power requirements, such devices have recently enjoyed widespread deployment in the form of lightweight sensors and RFID. Their deployment in the wild, and their mostly wireless communication abilities make them vulnerable to a wide variety of attacks, including (i) information snooping, (ii) inserting false or misleading information, (iii) jamming radio channels, (iv) making nodes run out of battery by never letting

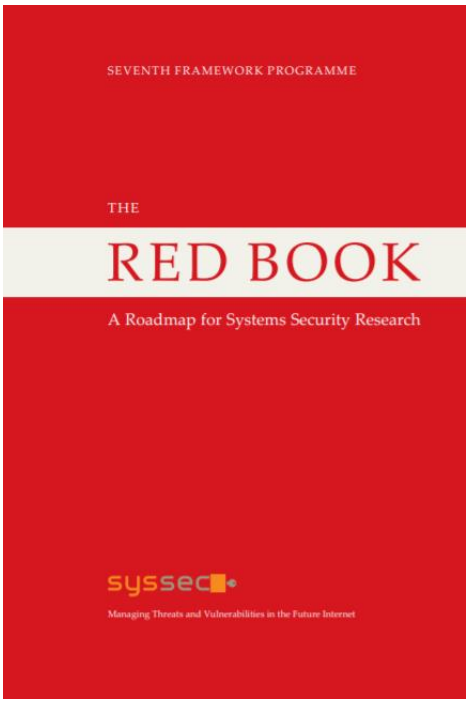
them sleep, (v) giving the impression of phantom nodes that do not exist, (vi) giving the impression of connectivity that does not exist, and (vii) making messages go through an attacking node that can selectively drop messages from the system. Mobile phones (and PDAs) also fall under this category of weak devices, and can also be a target for attacks including (i) mobile malware, (ii) eavesdropping, and (iii) DoS Attacks."

- "**Complexity**. Over the past years we have been building increasingly complex systems which, by definition, are more prone to errors and attacks. Since these systems are difficult, if not impossible, to model accurately, they are challenging to test and may lead to several threats, including: (i) unforeseen cascading effects, (ii) large-scale deployment of any attack, (iii) system parts that are vulnerable because of incomplete system maintenance, (iv) dormant functionality hidden in a program, and (v) race conditions and bugs due to the multi-threaded/parallel nature of applications."
- "**Data Manipulation**: more people, more data, more value. As more people use the internet, and as more organizations collect and store data on-line, we are bound to see an increasing number of attacks against (or based on) this data. The attacks may target several dimensions, including: (i) erosion of privacy due to ubiquitous sensors, (ii) false sensor data due to fabrication or falsification, (iii) data leaked from social networks, and (iv) data gathered from (or for) on-line games."
- "**Attack Infrastructure**. To launch large-scale attacks, several adversaries develop and deploy distributed offensive platforms (such as botnets), which serve as underground economy support structures serving (and operating on) advanced malware designed to evade detection and resist capture."
- "**Human Factors**. Humans are usually the weakest link in the security of several systems. Either as insider threats or as end-users, they may be the key element in the success of a cyberattack. Humans interact with security in several aspects including (i) user interfaces, which clearly convey a security (or lack thereof) to the user; (ii) insiders, who may have the access mechanisms needed to compromise a system; (iii) social engineering using all forms of communication, such as email, VoIP phones, and instant messaging systems; and (iv) targeted attacks on individuals or groups of people."
- "**Insufficient Security Requirements**. Some systems, such as legacy systems (sometimes deployed even before the deployment of the commercial internet), may have security requirements that are not adequate for the current time and scale."

II.3 The Red Book

The Red Book, a Roadmap for Systems Security Research, was produced as part of the SysSec Network for Excellence. SysSec mobilized the community in the area of systems security and came up with the most

important research challenges, (i) malware, (ii) targeted attacks, and (iii) social engineering – phishing, as well as the three most important domains of research: (i) mobile devices, (ii) social networks, and (iii) critical infrastructures.



The "Red Book" also outlined four "grand challenges" that need to be addressed [MB 2013]:

- **No Device Should Be Compromisable**: Develop the necessary hardware and software support to make it impossible for attackers to compromise a computer or communication device, including smartphones and tablets.
- **Give Users Control Over Their Data**: Provide the necessary mechanisms so that users (i) will be able to know which data they have created (such as text, photos, videos, cookies, web requests, etc.); (ii) will be able to know what data they have given to third parties (such as text, photos, cookies, web requests, IP addresses, etc.); (iii) will have the capability to refuse disclosure of some data (such as cookies and IP addresses) and still expect a decent level of service; (iv) will have the capability to delete their own data, which they have created (both from local storage and from the cloud); and (v) will, under an appropriate legal framework, also have the ability to ask past recipients of their data to erase them.
- **Provide Private Moments in Public Places**: Enable users to have private communication in the public areas of cyberspace. Consider the following analogy: The fact that people are having dinner in a public restaurant does not mean that their conversation could be recorded by the manager of the restaurant and later made available without their explicit consent. Similarly, the fact that people are communicating in cyberspace does not imply that parts of their communication can be recorded and used later through means outside their control. We propose to develop mechanisms that will enable people to have a reasonable expectation of privacy in what can be considered a public venue in cyberspace.
- **Develop Compromise-Tolerant Systems**: Provide adequate security levels even if components of the system have been compromised. It is reasonable to expect that not all attacks will be detected and successfully mitigated. Human errors, software errors, hardware errors and insufficient protection mechanisms will allow some attacks to go through successfully. This implies that some systems, or components of systems, will be compromised, and this may go undetected for a long period of time. Given such an environment, we should develop systems that will be able to provide decent security guarantees even if some of their components are compromised.

II.4 The SecUnity Roadmap

SecUnity, a project funded by the German Federal Ministry of Education and Research (BMBF) to support IT security research in Germany and Europe, produced its Roadmap for CyberSecurity Research in early 2019. The Roadmap defines three main categories: (i) Key Challenges, (ii) Interdisciplinary Challenges, and (iii) Technologies and Applications. The research areas identified in each of the three categories were:

- Key Challenges

    - Securing Cryptographic Systems against Emerging Attacks
    - Trustworthy Platforms
    - Secure Lifecycle despite Less Trustworthy Components
    - Quantifying Security
    - IT Security and Data Protection for Machine Learning
    - Big Data Privacy
- Interdisciplinary Challenges
    - Measurable, Risk-adequate Security in Law
    - Holistic Human-centred Security and Privacy Research
    - Digital Business Models for a Fair Economy and Society
- Technologies and Applications
    - Safeguarding Key Services of the Internet
    - Security of Blockchain Technology
    - Accountability and Transparency for Information Quality
    - User-centric Privacy Tools
    - Remotely Unhackable PC
    - IT Security for Autonomous Driving

II.5 The NESSOS Roadmap

NESSoS, the Network of Excellence on Engineering Secure Future Internet Software Services and Systems, elaborated a mid-term research roadmap that considered the relevant security challenges (new vulnerabilities and threats) that the adoption of the future internet could bring. Including these security challenges in the development of financial institutions' services meant the inclusion of security from early stages of the software development lifecycle (SDLC) when applied to software-based services and systems that belonged to the financial institution.

The roadmap focused on developing secure services for financial institutions. It addressed security at the service level, even when the infrastructure level must be considered to detect security requirements and constraints. Security at the hardware level or at the network level was of interest to NESSoS, mainly as a means of understanding the limitations it imposed on higher levels of abstraction for financial services. The NESSoS roadmap took into consideration the feedback and opinions of NESSoS partners but also of many other companies and institutions outside the consortium. In particular, feedback was sought from the so-called NESSoS community, composed of more than two hundred experts in the areas of cybersecurity and software engineering. The way that the roadmap tackled secure service development was by the typical process of gathering requirements, followed by the design of an architecture and ending in implementation. It is relevant to note that the proposal of the roadmap was to address security from the early phases of the SDLC, considering that security and privacy by design were main principles of NESSoS. However, it was noted that all of these might not be enough in the new settings that the financial institution might face. The services created needed to be secure. Therefore, security assurance was identified as a transversal topic to be considered of paramount importance. In addition, risk and cost awareness during the SDLC were transversals that formed one of the key research directions, since it linked security concerns with business and decision-making.

The roadmap also considered enabling methodologies and technologies that contributed to the enhancement of trustworthiness in financial institution services. It started with the methodologies usually involved in the SDLC, such as:

- Security requirements engineering
- Secure service architecture and design
- Security support in programming environments
- Service composition and adaptation
- Runtime verification and enforcement
- User-centric security
- Security management
- Autonomic security
- Quantitative aspects of security

Besides these topics, the NESSoS roadmap considered a set of crucial properties, such as compliance, privacy, trust and identity management, that had always to be taken into account.

Figure 26 shows a graphical representation of the topics listed above. In the core of this figure we depicted the major transversal topics of interest: security assurance and risk and cost-aware SDLC. Then, the topics highlighted in blue correspond to the software lifecycle (security requirements engineering, security service architectures and design, security support in programming environments, service composition and adaptation and runtime verification and enforcement). The four topics outside the inner box correspond to technologies that are related to the development of the lifecycle, but that emerged as additional topics of research (user-centric security, autonomic security, security management, quantitative aspects of security). The properties to be always enhanced and the threats to face are present in all the facets of the lifecycle (compliance, privacy, trust and identity management).

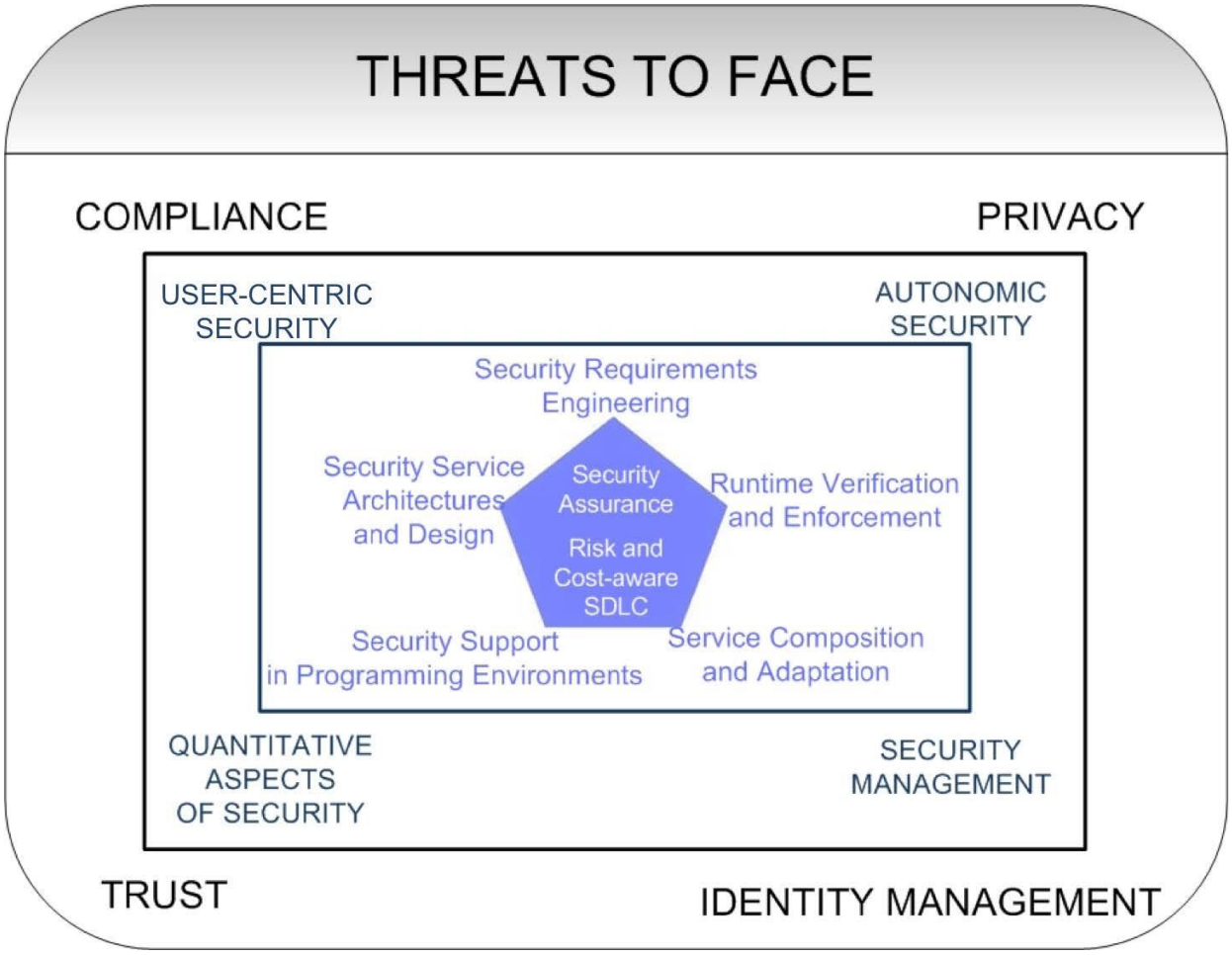


Figure 26: The Topics of the NESSOS Roadmap

II.6 The NIS WG3 SRA

The Working Group 3 (WG3), Secure ICT Research and Innovation, of the EU Platform on Network and Information Security (NIS), developed the first European Strategic Research Agenda (SRA) in the area of cybersecurity, in the period September 2013 – August 2015. It complemented and underpinned the EU NIS Strategy, and provided input to the secure ICT Research & Innovation agenda at national and EU levels, including the Horizon 2020 program.

The NIS WG3 SRA promoted the protection of three areas, as follows. Individual needs and fundamental rights, including social, legal and regulatory aspects of security and privacy; the collective interest of organized individuals, institutions and businesses in digital interconnected societies, including resilience; and ICT infrastructures that are meant to be adaptive, decentralized, collaborative, transparent and efficiently controlled, that must be safe, reliable, predictable and always available, and that must operate confidentially, protecting privacy by resisting and reacting to cyber incidents in real time.

The opportunities and recommendations to be addressed were grouped into four topics, namely research, policy, business, and education.

II.6.1 Research

After an initial cross-analysis of the different areas, the following research priorities emerged:

- Fostering assurance
- Focusing on data
- Enabling secure execution
- Preserving privacy
- Increasing trust
- Managing cyber risks
- Protecting ICT infrastructures
- Achieving user-centricity

II.6.1.1 Fostering assurance

Effective security means that security, privacy and trust considerations should be involved from the very beginning in the design of systems and engineering processes (security by design). This requires a combination of engineering, assessment and certification processes in a dynamic, synchronized, complete and effective approach. This process of enabling assurance techniques and processes can be definitely eased by policy regulators. A growing area identified as enabler is cyber insurance. This growing business area needs further research on security metrics and security assessment, as well as forensic and related technologies for establishing responsibilities in security incidents and attacks.

II.6.1.2 Focus on data

The increasing quantity, value and sensitivity of data, produced either by systems or by individuals, need to be effective protected. With data being stored and processed in the cloud, and being exchanged and shared between many previously unknown and unpredictable entities, this protection cannot stop at a single system's border, but must be applied to the data over its full lifecycle, regardless of which system is processing, accessing and controlling the data. Hence, a system-centric view, including, among other things, secure devices and infrastructures, needs to be complemented by a data-centric view, focusing on data lifecycle aspects by providing mechanisms that allow the data owner to control the usage of their data as a prerequisite of a secure and privacy-preserving digital life.

II.6.1.3 Enabling secure execution environment.

As a matter of fact, ICT based instruments depend on a secure execution environment and the respective software. Any loss of integrity in these elements is an opportunity for manipulation and possibly corruption. With more and more information being processed outside of secured premises, the need for secure execution environments and corresponding devices is rising. This holds for institutions in the public administration as well as for other critical infrastructures, such as the health care sector, smart grids, and industrial control systems for water, food/agriculture, nuclear and chemical operation. Secure execution environments are, then, even a critical factor for public safety and the provision of essential services.

II.6.1.4 Preserving privacy

Privacy has been considered as a central element in the three areas of interest from several perspectives. It is a basis of individual freedom and a cornerstone of society. The technologies to preserve and enable privacy should be available and easily understandable and deployable, especially in the big-data era. This demands new approaches to privacy engineering. In addition, research and innovation are needed to build technologies that allow users to separate their identities for different aspects of life, while research is also needed to deal with authentication in services that do not require a persistent identity.

II.6.1.5 Increasing trust

There is a growing need to develop for digital world relationships a set of norms, practices and behaviours that mimic and improve on those in the physical world. Algorithms and models should be developed for trust formation, evolution, aggregation and eventually dissolution. These models should consider evidence in several formats in order to develop certification models for trustworthiness.

II.6.1.6 Managing cyber risks

New developments in ICT technology and its applications are increasing the complexity of systems and provide a challenge for management. The increase in complexity is caused by the number of devices and components that are interconnected, the amount of data that is generated and processed, the number of people and objects that are interacting, the diverse protection needs of individuals and organizations, the variety in attacker motivations and targets, and more. Clearly, the time taken for detection, diagnosis, remediation planning and action is critical in limiting the impact of an attack. In the future, it can be expected that the sophistication and speed of execution of attacks will increase, and the difficulty of formulating a timely response will become correspondingly more challenging. A capability for autonomous response will become essential, because there will simply not be enough time to have a person in the loop. However, an inappropriate response may be more damaging than the original attack, so the controls need to be not only speedy, but also trustworthy. Despite the automation, people must remain in ultimate control, being able to set and modify policies that govern the actions of the autonomous agents. Establishing effective means of man-machine cooperation will be a research challenge in itself. Furthermore, network topology could morph dynamically to make itself harder to attack.

II.6.1.7 Protecting ICT infrastructures

We can observe that ICT infrastructures lie at the heart of many other hyperconnected infrastructures; thus, their protection should be a predominant concern. While the term is broad, several areas have been identified, such as networks, clouds and mobile devices, where further progress is necessary. Without security in the core infrastructure, no other layer would be secure.

II.6.1.8 Achieving user-centricity

If privacy protection demands that users be in control of their data and that systems and services provide transparency concerning their data processing, users need to be able to express their preferences and to assess the risk associated with decisions they make with respect to their data. Users need to be empowered to manage their digital identities by defining their policies and preferences in an intuitive way. While many aspects of systems and services related to security and privacy can already be technically accessed, configured and maintained today, such configurations and maintenance should not be manageable only by technology experts. With the increased penetration of ICT, everyone must be able to do so. How this can be achieved while technology continues to become more complex, remains a challenge. Meeting this challenge is a prerequisite for avoiding a digital divide.

There is a wide range of publications that provide specific coverage of the cybersecurity research and innovation ecosystem, timescales and asymmetry. All offer recommendations that may be summarized as follows:

- Experimental cybersecurity research is needed to shift the asymmetric cyberspace context to one of greater planning, preparedness and solutions that offer a higher level of assurance.

- Emphasis on isolated and niche equipment and related software solutions alone will fall far short of achieving the transformational shift in research, community and supporting experimentation that is required to address cybersecurity in the ever-escalating cyber environment.
- Strong, coupled and synergistic advances in fundamental methodological development, fostering and leveraging communities of researchers and advancing the capabilities of the infrastructure supporting that research, will move the field beyond today's state of the art.
- Support for cross-domain and multidisciplinary experimentation is recommended: this includes computer science, engineering, math/modelling, human behaviour, sociology and economics. The views, perceptions and behaviours of the different fields cannot be ignored, because they could be decisive factors in obtaining optimal results.
- The portability of experiments, packaged for sharing and reuse in cross-discipline experiments, is important and also enhances their effectiveness.

II.6.2 Policy

NISP WG3 constituents identified that policies in the NIS and privacy domains should:

- act as enablers to support research and innovation, and
- set the targets that researchers and industry should aim for.

Guided by these two principles, the following were proposed as areas of focus for NIS policy making.

- European cybersecurity and privacy cooperation and governance
- Balancing cybersecurity and privacy requirements
- Mitigating the concentration of strategic cybersecurity resources and technologies outside Europe
- Critical infrastructure protection

II.6.3 Business

A sub-group of WG3 examined the requirements for NIS research and innovation from the perspective of European end-user organizations and providers of products and services – essentially the demand- and supply-side stakeholders in the NIS market-place.

The current situation was one of unsatisfied demand. The incidence and impact of security breaches were increasing, cybersecurity was already an issue in many boardrooms, and consequently expenditure on security products and services was rising (by around 8% year on year according to Gartner). There is no shortage of products on the market. Yet, already at that time there was a significant gap between what end-user organizations needed, and what the NIS industry could provide.

The key aspects to develop were then listed as follows.

- A systems approach to security
- Innovative models for cybersecurity products and services
- New approaches to the mismatch of research and innovation timescales, e.g. with agile R&I sandboxes
- Harmonized regulation, information sharing and behavioural research

II.6.4 Education

Three major educational challenges were identified:

- Education on privacy and related issues adapted to stakeholders
- Clarification of the responsibility for continuous education and raising awareness campaigns
- Bringing massively open online courses (MOOCs) to the same level as real-life in-class courses, from the perspectives of quality and certification

The key aspects in cybersecurity education were depicted as:

- Multi-disciplinary focus
- A dynamic approach to teaching cybersecurity skills, adapted to changes in technology and societal environment
- Alignment of curricula and training with demand for skills
- Using appropriate methodologies for teaching cybersecurity at all levels, from awareness to focused expertise
- Ensure that all member states attain the same level regarding indicators of cybersecurity skills

II.7 Relation to this work

All the roadmaps described above have been very useful and have influenced cyber security research in one way or another. In their development, they all appear to share a common dimension: they focus on "horizontal" research directions, that is, research directions that can be applied in several different application areas. In this aspect, these roadmaps propose the development of "tools" and "mechanisms" that applications will probably use at a later stage in order to improve their cyber security posture.

In this work, however, we follow a complementary approach: We first go to the applications (i.e. the verticals) and ask them: "What kinds of tools do you need? What kind of cybersecurity research would be important for your application?". In this aspect our work is much more focused. Application stakeholders explicitly state their needs and we define the cybersecurity research challenges that need to be addressed in order to satisfy the needs of the vertical stakeholders. As a result, the research challenges that this roadmap proposes are of immediate use (to the verticals) as they are the result of the consultation with the application stakeholders. On the other hand, however, we should admit that there can be research areas that can be considered important but are just not needed in the verticals we considered.

Annex III References

[AGK 2019] Ahmed Amro, Vasileios Gkioulos, Sokratis Katsikas, Connect and Protect: Requirements for Maritime Autonomous Surface Ship in Urban Passenger Transportation, 5th Workshop on the Security of Industrial Control Systems & of Cyber-Physical Systems (CyberICPS 2019)

[BBWMLSF 2013] W. Bruhn, H. C. Burmeister, L. Walther, J. Moræus, M. Long, M. Schaub, and E. Fentzahn. Munin d5.2: Process map for autonomous navigation. Technical report, 2013.

[Bernabe 2019] Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T., & Skarmeta, A. (2019). Privacy-preserving solutions for Blockchain: review and challenges. *IEEE Access*, *7*, 164908-164940.

[BWMLSF2015] H.-C. Burmeister, W. Bruhn, L. Walther, J. A. Moræus, and B. Sage-Fuller. Munin d8.6: Final report: Autonomous bridge. Technical report, 2015.

[BFMNRLS 2018] Bernsmed K, Frøystad C, Meland PH, Nesheim DA, Rødseth ØJ Visualizing Cyber Security Risks with Bow-Tie Diagrams. In: International Workshop on Graphical Models for Security, 2017. Springer, pp 38-56.

[BIZJAK 2019] T. BIZJAK, "Sacramento, Calif., Transit System Recovers from Ransomware Attack," 22 November 2017. [Online]. Available: https://www.govtech.com/security/Sacramento-Calif-Transit-System-Recovers-from-Ransomware-Attack.html. [Accessed 18 December 2019].

[Brewster 2016] T. Brewster, "Ransomware Crooks Demand $70,000 After Hacking San Francisco Transport System," 2016. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2016/11/28/san-francisco-muni-hacked-ransomware/. [Accessed 18 December 2019].

[Cambell 2015] Campbell, B., Jones, M., & Mortimore, C. (2015). Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants.

[Casey 2007] T. Casey, "Threat Agent Library Helps Identify Information Security Risks.," INTEL 10.13140/RG.2.2.30094.46406. , 2007.

[Cavoukian 2019] A. Cavoukian, “Privacy by Design: The 7 Foundational Principles,” June 2013. [Online]. Available: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf. [Accessed 3 December 2019].

[Clang10] Clang 10 - Control Flow Integrity, https://clang.llvm.org/docs/ControlFlowIntegrity.html. Clang 10 - SafeStack, https://clang.llvm.org/docs/SafeStack.html

[CER 2019] C. Cerrudo, "An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks," 2015. [Online]. Available: https://ioactive.com/pdfs/IOActive_HackingCitiesPaper_CesarCerrudo.pdf. [Accessed 2 December 2019].

[COMPACT 2018] COMPACT Project, "Overall COMPACT architecture," (H2020 Project, G.A.740712), 2018.

[CYBER 2005] E. Lazowska, Cyber security: A crisis of prioritization, PRESIDENT'S INFORMATION TECHNOLOGY ADVISORY COMMITTEE ARLINGTON VA., 2005.

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

[DECLERCQ 2002] De Clercq, J. (2002, October). Single sign-on architectures. In International Conference on Infrastructure Security (pp. 40-58). Springer, Berlin, Heidelberg.

[Deere 2018] S. Deere, "CONFIDENTIAL REPORT: Atlanta's cyber attack could cost taxpayers $17 million," *The Atlanta Journal-Constitution,* 1 August 2018.

[Deloitte 2019] Deloitte Insights, "Making smart cities cybersecure," 2019.

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

[EISAC 2016] E-ISAC, Analysis of the Cyber Attack on the Ukrainian Power Grid, 2016

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

[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. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/EDPS_10_6. [Accessed 3 December 2019].

[ENISA 2017] ENISA, "Baseline Security Recommendations for IoT, in the context of Critical Information Infrastructures," 2017.

[ENISA 2018] ENISA, "Good Practices for Security of Internet of Things, in the context of Smart Manufacturing," 2018.

[ENISA 2019] PORT CYBERSECURITY: Good practices for cybersecurity in the maritime sector. 2019.

[ENISA 2019A] ENISA, Industry 4.0 Cybersecurity: Challenges & Recommendations, May 2019, (last access in December 2019).

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

[FBM 2017] Christian Frøystad, Karin Bernsmed and Per Håkon Meland. Protecting Future Maritime Communication. In Proceedings of The 12th International Conference on Availability, Reliability and Security (ARES'17), Reggio Calabria, Italy — August 29 - September 01, 2017. Association for Computing Machinery (ACM) 2017 ISBN 978-1-4503-5257-4.

[Ferreira et al, 2017] Ferreira, H., Silva, F., Sousa, P., Matias, B., Faria, A., Oliveira, J., ... & Silva, E. (2017, September). Autonomous systems in remote areas of the ocean using BLUECOM+ communication network. In OCEANS 2017-Anchorage (pp. 1-6). IEEE.

[HACKREAD 2019] HACKREAD, "Baltimore' 911 CAD system hacked; remained suspended for 17 hours," 28 March 2018. [Online]. Available: https://www.hackread.com/baltimore-911-cad-system-hacked-suspended/. [Accessed 02 December 2019].

[HARDT 2012] Hardt, D. (2012). The OAuth 2.0 authorization framework.

[HHKSR 2017] M. Höyhtyä, J. Huusko, M. Kiviranta, K. Solberg and J. Rokka, "Connectivity for autonomous ships: Architecture, use cases, and research challenges," in 2017 International Conference on Information and Communication Technology Convergence (ICTC), 2017.

[HOMRJ 2017] M. Höyhtyä, T. Ojanperä, J. Mäkelä, S. Ruponen and P. 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, 2017.

[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.

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

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

[IMO 2004] International Maritime Organization. SOLAS chapter XI-2

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

[JRC 2019] I. NAI-FOVINO, R. NEISSE, J. L. HERNANDEZ-RAMOS, N. POLEMI, G. RUZZANTE, M. FIGWER and A. LAZARI, "A Proposal for a European Cybersecurity Taxonomy," JRC, 2019.

[KA 2019] L. Kearney and L. Adler, "Atlanta officials reveal worsening effects of cyber attack," 7 June 2018. [Online]. Available: https://www.reuters.com/article/us-usa-cyber-atlanta-budget/atlanta-officials-reveal-worsening-effects-of-cyber-attack-idUSKCN1J231M. [Accessed 2 December 2019].

[KAMZ 2019] G. Kambourakis, M. Anagnostopoulos, W. Meng and P. Zhou, Botnets: Architectures, Countermeasures, and Challenges, CRC Press, 2019.

[KKG 2018] Georgios Kavallieratos, Sokratis Katsikas, and Vasileios Gkioulos. Cyber-attacks against the autonomous ship. In SECPRE 2018, CyberICPS 2018. Lecture Notes in Computer Science, vol 11387, pages 20–36. Springer, 2018.

[KLNT2011] D. Kokotos, D. Linardatos, N. B. Nikitakos, and E. S. Tzannatos. Information and communication technologies in shipping industry (In Greek), 2011.

[LGPP 2010] H.-M. Lin, Y. Ge, A.-C. Pang and J. S. Pathmasuntharam, "Performance study on delay tolerant networks in maritime communication environments," in OCEANS'10 IEEE, SYDNEY, 2010.

[LDC 2013] L. Lambrinos, C. Djouvas and C. 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), 2013.

[LSS 2011] Lund, M.S., Solhaug, B., Stølen, K.: Model-driven risk analysis – The CORAS approach. Springer (2011).

[L 2016] Lloyds Register. Cyber-enabled ships. page 20, 2016.

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

[MBFLS 2018] Meland PH, Bernsmed K, Frøystad C, Li J, Sindre G (2018) An Experimental Evaluation of Bow-Tie Analysis for Security. In: Computer Security. Springer, pp 173-191.

[MICROSOFT 2009] Microsoft. The stride threat model, 2009.

[MITIGATE 2017] MITIGATE project. Deliverable D4.4" Integrated MITIGATE System, 2017.

[MUNIN 2016] MUNIN. Maritime unmanned navigation through intelligence in networks, 2016.

[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 2018] NIST, Framework for Improving Critical Infrastructure Cybersecurity, v1.1, April 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (last access in December 2019).

[NIST 2019] NIST, Cyber Supply Chain Risk Management, 2019 https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management (last access in December 2019).

[NR2017] H. Nordahl Ø. J. Rødseth. Nfas-definitions for autonomous merchant ships. 10 2017.

[Paul 2017] Paul Voigt and Axel von dem Bussche. 2017. The EU General Data Protection Regulation (Gdpr): A Practical Guide (1st ed.). Springer Publishing Company, Incorporated.

[Pawloski et al, 2017] Andre Pawloski, Moritz Contag, Thorsten Holz, Victor van der Veen, Chris Ouwehand, Herbert Bos, Elias Athanasopoulos, and Cristiano Giuffrida. In Proceedings of the 24th Network and Distributed System Security Symposium (NDSS). San Diego, CA, US, February 2017

[RJ] DK Rasmus, Nord Jorgensen, in Copenhagen. Bimco: The guidelines on cyber security onboard ships. Available online at: https://iumi.com/news/blog/bimco-the-guidelines-on-cyber-security-onboard-ships.

[RN2017] Rødseth, Ø., Nordahl, H., Definitions for autonomous merchant ships. In: Norwegian Forum for Unmanned Ships (2017

[RNH 2018] Ørnulf Jan Rødseth, Havard Nordahl, and Asa Hoem. Characterization of autonomy in merchant ships. In 2018 OCEANS-MTS/IEEE Kobe Techno-Oceans (OTO), pages 1–7. IEEE, 2018

[RT2014] Rødseth, Ø.J., Tjora, Å., A system architecture for an unmanned ship. In: Proceedings of the 13th International Conference on Computer and IT Applications in the Maritime Industries (COMPIT) (2014)

[RR 2016] Rolls-Royce. Remote and autonomous ship-the next steps. page 88, 2016.

[Seattle 2019] Seattle Office and Emergency Management, "7.3 Cyber Attack and disruption," in *SEATTLE HAZARD IDENTIFICATION AND VULNERABILITY ANALYSIS*, Seattle, 2019.

[SFAR2015] M. Schmidt, E. Fentzahn, G. F. Atlason, and H. Rødseth. Munin 8.7 final report autonomous engine room. Technical report, 2015.

[Sarbinowski et al, 2016] Pawel Sarbinowski, Vasileios P. Kemerlis, Cristiano Giuffrida, and Elias Athanasopoulos. In Proceedings of the 32nd Annual Computer Security Applications Conference (ACSAC). Los Angeles, CA, US, December 2016.

[Skarmeta 2019] CyberSec4Europe Deliverable D3.1 Common Framework Handbook 1 CyberSecurity 4 Europe project. Editor Antonio Skarmeta. 2019.

[Truman 2003] Truman, G. E., Sandoe, K., & Rifkin, T. (2003). An empirical study of smart card technology. *Information & Management*, *40*(6), 591-606.

[van der Veen et al, 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.

[WGSJGABMWN2018] Wimpenny, Gareth & Safar, Jan & Grant, Alan & Bransby, Martin & Ward, Nick. (2018). Public Key Authentication for AIS and the VHF Data Exchange System (VDES). 1841-1851. 10.33012/2018.15948.