# Stakeholder perspectives and requirements on cybersecurity in Europe

Simone Fischer-Hübner, Cristina Alcaraz, Afonso Ferreira, Carmen Fernandez-Gago, Javier Lopez, Evangelos Markatos, Lejla Islami, Mahdi Akil

Journal of Information Security and Applications 61 (2021) 102916

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

# Stakeholder perspectives and requirements on cybersecurity in Europe

Simone Fischer-Hübner [a,*], Cristina Alcaraz [b], Afonso Ferreira [c], Carmen Fernandez-Gago [b], Javier Lopez [b], Evangelos Markatos [d], Lejla Islami [a], Mahdi Akil [a]

[a] Karlstad University, Department of Mathematics and Computer Science, Karlstad, Sweden
[b] University of Malaga, Computer Science Department, Malaga, Spain
[c] CNRS (Centre National de La Recherche Scientifique), Toulouse, France
[d] FORTH (Foundation for Research and Technology - Hellas), Heraklion, Greece

ARTICLE INFO

*Keywords:*
Cybersecurity
Requirements
Stakeholder engagement
Research & innovation roadmap

ABSTRACT

This article presents an overview and analysis of the key cybersecurity problems, challenges and requirements to be addressed in the future, which we derived through 63 interviews with European stakeholders from security-critical sectors including Open Banking, Supply Chain, Privacy-preserving Identity Management, Security Incident Reporting, Maritime Transport, Medical Data Exchange, and Smart Cities. We show that common problems, challenges and requirements across these sectors exist in relation to building trust, implementing privacy and identity management including secure and useable authentication, building resilient systems, standardisation and certification, achieving security and privacy by design, secure and privacy-compliant data and information sharing, and government regulations. Our results also indicate cybersecurity trends and allow to derive directions for future research and innovation activities that will be of high importance for Europe.

## 1. Introduction

Facing steadily increasing cybersecurity challenges, the European Commission has been committed to enhance its cybersecurity competence in member states and in its institutions. The CyberSec4Europe project[1] belongs, together with CONCORDIA,[2] ECHO[3] and SPARTA,[4] to the EU Commission's four H2020 pilot projects for establishing and operating a European Cybersecurity Competence Network.

CyberSec4Europe has as its main objective to test and demonstrate potential governance structures for a network of competence networks and centres using the best practice examples from the expertise and experience of the participants. Its project demonstration use cases address cybersecurity challenges within seven areas that have been defined in the project as important security critical sectors: *Open Banking, Supply Chain, Privacy-preserving Identity Management (IDM), Security Incident Reporting, Maritime Transport, Medical Data Exchange, and Smart Cities.*

The sectors open banking, supply chain, maritime transport, medical data exchange and smart cities were chosen as they represent important critical information infrastructure areas for finance, health, transport, and other essential private and governmental services. Moreover, they are heavily relying on IoT (Internet of Things) and modern communication technologies (including 5G), which pose serious security challenges. The EU Commission therefore also identified these areas as essential areas to be addressed by its recently published Cybersecurity Strategy [1]. In addition, the sectors of privacy-preserving IDM and security incident reporting are relevant for implementing privacy by design and security response, and thus for enforcing the EU Legal Privacy and Cybersecurity framework including the EU General Data Protection Regulation (GDPR) [2] and the Directive on Security of Network and Information Systems (NIS Directive) [3]. For these reasons, we have chosen these security-critical sectors as a basis for addressing our research objective of analysing stakeholders' perspectives and requirements on cybersecurity in Europe. This analysis of stakeholders' perspectives and requirements also serves as an input for analysing the need for innovative and multidisciplinary research into cybersecurity for these sectors, and based on this, for developing a common European Cybersecurity Research and Innovation (R&I) Roadmap for security critical sectors by the CyberSec4Europe project.

* Corresponding author.
*E-mail address:* simone.fischer-huebner@kau.se (S. Fischer-Hübner).

[1] https://cybersec4europe.eu/.
[2] https://www.concordia-h2020.eu/.
[3] https://echonetwork.eu/.
[4] https://www.sparta.eu/.

https://doi.org/10.1016/j.jisa.2021.102916

To this end, we conducted qualitative and exploratory research through structured interviews with 63 key stakeholders, including industrial, governmental and academic representatives, from all seven sectors and from different European countries.

In this article, we present the results from our interviews for addressing the research objectives of (a) analysing the perspectives on *key problems* that stakeholders are facing for the sectors that they represent and *challenges* for cybersecurity, especially for the mid and long-term, and of (b) eliciting their cybersecurity *requirements* in terms of capabilities and technologies which will allow to lay the foundation for the R&I roadmap.

As one of its main contributions, this article provides a unique snapshot of the cybersecurity problem space and related requirements as described by European cybersecurity experts, including both practitioners and researchers. The elicited problems, challenges and requirements, which are also impacted by the European regulatory framework and guidelines from European institutions, show essential trends and directions for future European cybersecurity research and innovation activities that will be important to address and will potentially have a high impact on science, industry and society in Europe. To this end, this article also provides important insights for implementing the EU Commission's cybersecurity strategy.

The remainder of this article is structured as follows: Section 2 briefly presents related previous work cybersecurity roadmaps and landscapes in Europe and compares it with our work. Section 3 discusses our research methodology for eliciting and analysing the stakeholders' perspectives and requirements. The results of our interviews for the seven security critical sectors are then presented in Section 4. Section 5 highlights key problems and challenges and requirements that the different sectors have in common and shows how these commonalities have become one of the foundations for the initial R&I roadmap of CyberSec4Europe. Finally, Section 6 outlines the conclusions that can be drawn from our work for ongoing and future cybersecurity research and innovation activities.

## 2. Related work

Over the past decade we have seen the rise of several landscapes and roadmaps in the area of cybersecurity [4–6]. Probably the first highly-influential roadmap was "CyberSecurity: A crisis of prioritization" [7]. This roadmap argued for more funding for civilian security research, urged for more engagement in basic (or fundamental) research, and outlined several research directions: authentication, software engineering, software assurance, monitoring, detection, mitigation, recovery, etc. More recently, the SysSec Network of Excellence published "The Red Book: A Roadmap for Systems Security Research" [8]. In this Red Book, the Systems Security community outlined the systems where cybersecurity will be important: social networks, critical infrastructures, legacy systems, mobile devices, etc.

After that, the NIS Platform published their research agenda [9], and eventually ECSO (The European Cyber Security Organisation) started publishing their Strategic Research and Innovation Agenda, which is now in its third edition [10]. Although the "Red Book" and the "Crisis of Prioritization" involve mostly the views of the academic community, ECSO is industry-driven and to a great extent reflects the view of the industry. As a result, we see a special focus on industry, supply chain, security by design, as well as certification and standardisation. The European Commission's Joint Research Center has recently published their "on Anchor Report" where they identify challenges in the digital landscape.[5] Europol also publishes their yearly IOCTA (Internet Organized Threat Assessment) Report where they list the most important challenges in the area of cybercrime (and cybersecurity).[6] Among other challenges, they identify payment fraud, the dark web, and cyber-dependent crime as the top priorities. Finally, several projects, including cyberwathcing.eu,[7] SPARTA,[8] and SecUnity[9] have recently published their roadmaps that focus on the area of cybersecurity, which were either created based on existing roadmaps or workshops involving European researchers. In contrast, for our work to prepare the CyberSec4Europe R&I roadmap, we have considered the viewpoints from stakeholders that we interviewed coming from industry, government and academia, and coming mainly from different security-critical sectors.

In addition to the above "horizontal" approaches, there exist several studies that focus on the security aspects of specific vertical areas. For example, [11] focuses on unoccupied aerial systems (such as drones) and identifies several research challenges including trustworthiness, monitoring, and resilience. Similarly, [12] addresses attacks on autonomous vehicles, and focuses on attacks related to machine learning. Nader et al. [13] focus on smart cities and argue that a data-driven approach would significantly improve the security posture of smart cities.

Other studies focus on geographical regions such an individual countries. For example, [14] focuses on the cybersecurity challenges of the Croatian society in the wake of its joining the European Union. Several geographically-focused studies and strategies have also been collected by ENISA.[10]

Finally, some other studies focus on specific age groups. For example [15] focuses on cybersecurity challenges for children, clearly demonstrating how unrestricted access may expose children to danger.

Our work shares many of the goals of this previous work. Indeed, we both would like to know what should be a roadmap for the future. On the other hand, our work presents an important snapshot: the point of view of the stakeholders. Therefore, this paper presents not what the researchers would like to work on, but what key cybersecurity stakeholders with different backgrounds think.

In contrast to the Threat Landscape published by the European Network and Information Security Agency (ENISA) [16] that also considers stakeholders' views in addition to media reports, our snapshot also analyses mid- and long-term cybersecurity challenges and requirements beyond immediate technical security threats. To the best of our knowledge, this aspect is unique and should provide a valuable insight.

## 3. Methodology

### 3.1. Choice of methodology and set-up

Interviews were chosen as an instrument to conduct qualitative and exploratory research based on detailed and qualitative data that we obtained, which allowed us to receive more detailed explanations and deeper insights into cybersecurity problems, challenges and requirements. As a data collection method we used structured interviews based on a protocol defining the exact wording and sequence of five questions (listed in Fig. 1), which resulted in the interviewers asking each participant exactly the same questions in the same order. Even though we used structured interviews, our choice of open-ended question still allowed to collect qualitative data.

The purpose of the first question Q1 was to collect demographic data in a form allowing us to anonymise the results to be published

[5] https://publications.jrc.ec.europa.eu/repository/handle/JRC121051.

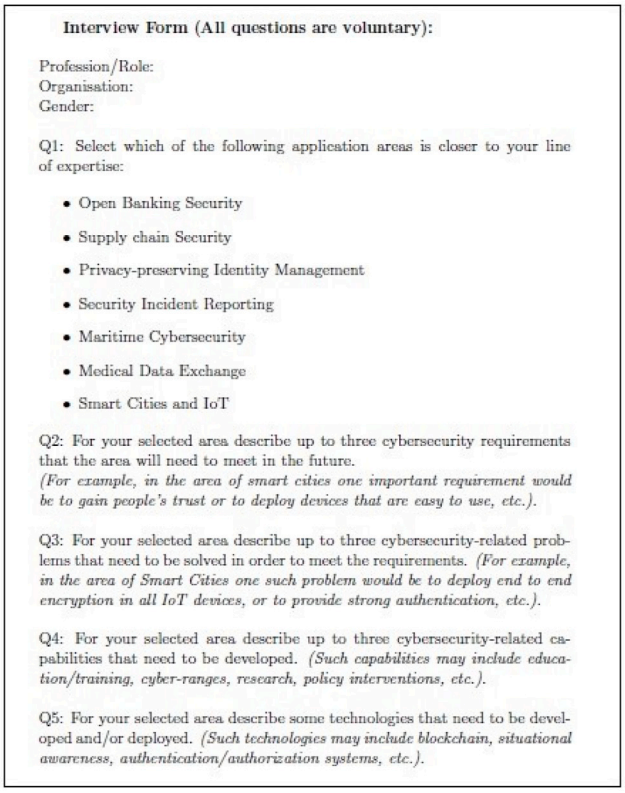
[6] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020.

[7] https://cyberwatching.eu/d44-eu-cybersecurity-privacy-interim-roadmap.

[8] https://www.sparta.eu/assets/deliverables/SPARTA-D3.2-Updated-SPARTA-SRIA-roadmap-v1-PU-M12.pdf.

[9] https://it-security-map.eu/en/roadmap/secunity-roadmap/.

[10] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.



**Interview Form (All questions are voluntary):**

Profession/Role:
Organisation:
Gender:

Q1: Select which of the following application areas is closer to your line of expertise:

- Open Banking Security
- Supply chain Security
- Privacy-preserving Identity Management
- Security Incident Reporting
- Maritime Cybersecurity
- Medical Data Exchange
- Smart Cities and IoT

Q2: For your selected area describe up to three cybersecurity requirements that the area will need to meet in the future.
*(For example, in the area of smart cities one important requirement would be to gain people's trust or to deploy devices that are easy to use, etc.).*

Q3: For your selected area describe up to three cybersecurity-related problems that need to be solved in order to meet the requirements. *(For example, in the area of Smart Cities one such problem would be to deploy end to end encryption in all IoT devices, or to provide strong authentication, etc.).*

Q4: For your selected area describe up to three cybersecurity-related capabilities that need to be developed. *(Such capabilities may include education/training, cyber-ranges, research, policy interventions, etc.).*

Q5: For your selected area describe some technologies that need to be developed and/or deployed. *(Such technologies may include blockchain, situational awareness, authentication/authorization systems, etc.).*

**Fig. 1.** Questionnaire with interview questions.

and to identify the application area and professional background of the interviewee for which the answers will apply. Questions Q2 to Q5 directly match our objectives to collect their general requirements (Q2), to help them define their important problems and challenges (Q3) and to lay the foundation for the roadmap (Q4 in terms of requirements for capabilities, Q5 in terms of requirements for technologies). In order to keep interviews short and focused, the questions were restricted to this set. The questions were formulated to allow us to analyse and elicit future, including mid- and long-term, challenges and requirements.

The instrument of structured interviews allowed us to gather consistent and comparable data and to reduce biases and inconsistencies that are more likely to be introduced with unstructured or semi-structured interviews [17,18], especially if (as in our case) different interviewers are involved that could ask different freely formulated questions in different ways. Moreover, structured interviews are faster to execute than unstructured or semi-structured interviews, as the questions are restricted to the ones defined in the interview protocol. This also motivated our choice, since the targeted key stakeholders usually had time-restrictions and we therefore planned to limit the interviews to a duration of not more than 20–30 min.

The interview set-up and research plan was reviewed and approved by one of the Ethical Advisors at Karlstad University (for more details, see [19]).

### 3.2. Data collection

In total, 63 interviews were conducted by the project partners from May until the end of June 2019. The (pseudonymised) interviewees per sector area with their respective backgrounds are listed in Table 1. Both key researchers and practitioners coming from industry, government or academia were involved for reflecting different perspectives and experiences.

The volunteering interviewees were recruited via professional contact networks of the partners and received an invitation letter explaining the objectives and set-up of the interviews together with an informed consent form to be signed by all interviewees.

Interviews were usually conducted either in person or via telephone conference and took on average between 20 and 30 min. The interviewer participated in the interview usually together with one or two assisting researchers. All of them took notes.[11]

If the interviewees consented, the interviews were audio recorded, which allowed us to go back to the interview session recordings later for comparing or verifying the notes with them. All participating researchers wrote down the main responses and key findings from the interviews based on their notes and after cross-checking with audio recordings if they were available.

Some of the interviewees also provided written answers to the questions, which they could then present and complement in a subsequent interview.

### 3.3. Data evaluation

In the next round, the interviewers combined all results and findings for a specific application area (sector) from the interviews from all note takers into one document. Proposed corrections, revisions and interpretations in the second round were discussed among the team of interviewer and assistants and cross-checked with the audio recordings (if available).

For each sector, all interviewers and assistants (2 or 3 per sector) then reviewed the collected data by marking main statements, analysing patterns or repeated statements and ideas that emerged and then categorising the data accordingly for deriving the main findings per sector. In joint discussions with all interviewers and assistants, inconsistency were discussed, resolved and agreements on the main categorisations and findings per sector were achieved.

Finally, an analysis was conducted in a consolidating discussion workshop by the team of all interviewers for jointly discussing and deciding on the key findings in a consistent manner across sectors and discussing commonalities.

The four phases of interviewing, combining notes, analysis and categorisation per sector and final analysis for deriving commonalities and agreeing on main findings are illustrated in Fig. 2.

## 4. Results: The stakeholder perspectives and requirements

In this section, we briefly introduce each of the seven security-critical sectors and summarise the key problems and challenges as well as the requirements that we elicited from the stakeholder interviews for these respective sectors. Problems and challenges were mainly identified based on the answers to question Q3, while general requirements as well as requirements in terms of capabilities and technologies that need to be developed or deployed were elicited based on the answers to questions Q2, Q4, and Q5.

### 4.1. Open banking

The context in this area is underpinned by the EU Payment Services Directive 2 (PSD2) [20] that is in force since the 13th of January 2018, enabling bank customers to use third-party providers to manage their finances, pay their bills, make peer-to-peer transfers, and analyse their spending, while still having their money safely placed in their current bank account. Banks are obligated to provide these third-party providers access to their customers' accounts through open APIs (Application Program Interfaces), allowing third-parties to build financial services on top of banks' data and infrastructure.

[11] Notes from the interviews and findings are published in a project report [19].

**Table 1**
List of stakeholders interviewed including the pseudonyms used to refer to them in the text, their sectors and professional backgrounds.

| ID (Pseudonym) | Sector | Professional background |
|---|---|---|
| #p1 | Open banking | Communications and marketing unit |
| #p2, p3, p5 | Open banking | Cybersecurity expert |
| #p4 | Open banking | Consulting manager |
| #p6, p7, p11–13, p15, p16, p18 | Supply chain | IT-Security expert |
| #p8, p14, p20, p21 | Supply chain | Cybersecurity expert |
| #p9 | Supply chain | Cybersecurity consulting expert |
| #p10 | Supply chain | Researcher |
| #p17 | Supply chain | Security certification expert |
| #p19 | Supply chain | Software expert |
| #p22 | Privacy-preserving IDM | Crypto expert from Industrial Research Lab |
| #p23 | Privacy-preserving IDM | Crypto expert from National Research Lab |
| #p24 | Privacy-preserving IDM | Data unit security manager |
| #p25 | Privacy-preserving IDM | Researcher |
| #p26 | Privacy-preserving IDM | Cybersecurity researcher and innovation booster |
| #p27 | Privacy-preserving IDM | Cybersecurity director |
| #p28 | Privacy-preserving IDM | Cybersecurity sales manager |
| #p29, p30 | Privacy-preserving IDM | Cybersecurity expert |
| #p31 | Privacy-preserving IDM | Faculty manager (service support to product delivery) |
| #p32 | Incident reporting | Data security unit manager |
| #p33 | Incident reporting | Information security officer |
| #p34 | Incident reporting | Communications and marketing expert |
| #p35 | Incident reporting | Intelligence analyst |
| #p36 | Incident reporting | Cyber threat intelligence expert |
| #p37 | Incident reporting | Army officer — Signals expert |
| #p38 | Incident reporting | Cybersecurity sales manager |
| #p39 | Incident reporting | Private Computer Security Incident Response Team (CSIRT) staff |
| #p40 | Incident reporting | Senior consultant expert |
| #p41, p42 | Incident reporting | Cybersecurity expert |
| #p43, p46 | Maritime transport | Researcher - Expert |
| #p44 | Maritime transport | Researcher - Project coordinator |
| #p45 | Maritime transport | Chief financial officer |
| #p47 | Medical data exchange | IT-Security manager |
| #p48 | Medical data exchange | Professor |
| #p49 | Medical data exchange | Software engineer |
| #p50 | Medical data exchange | Security certification expert |
| #p51 | Medical data exchange | Entrepreneur and early stage investor |
| #p52 | Medical data exchange | Chief information security officer - Hospital |
| #p53 | Medical data exchange | Consulting manager |
| #p54 | Medical data exchange | Cybersecurity director |
| #p55 | Medical data exchange | Cybersecurity sales manager |
| #p56 | Smart cities | Cybersecurity expert |
| #p57, p58 | Smart cities | Researcher/Engineer |
| #p59 | Smart cities | Senior researcher |
| #p60–p63 | Smart cities | Researcher |

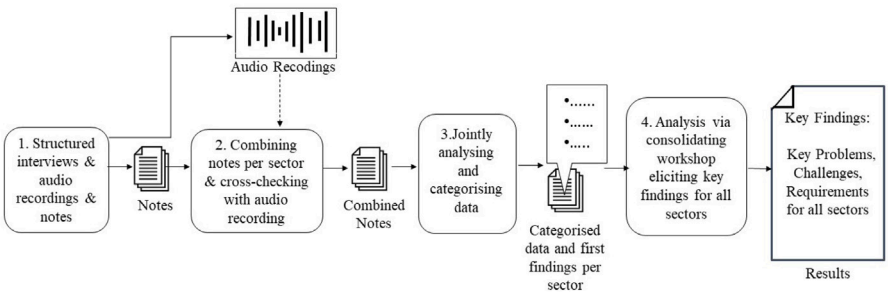



**Fig. 2.** Phases of data collection and analysis.

#### 4.1.1. Key problems and challenges

This migration to open environments considerably increases the cybersecurity threat landscape [21]. Three critical issues currently require both a significant change in the practice of cybersecurity and the construction of technological innovations in this area, as follows:

- **Professional threats**. Threats are increasingly professional and easy to copy and repeat by cyber criminals.
- **Real time threats.** The evolution of consumer banking toward ever more real time transactions will limit the ability of banking players to react efficiently in the event of proven fraud.

- **API security risks**. Banking information systems architectures have been deeply remodelled, now focusing on APIs as critical business components.

The key challenges stated in the 5 interviews that we conducted were accordingly related to fraud detection, including identity management and threat intelligence, including threat data-sharing, as follows:

- Interviewees #p2, p3, and p5 emphasised the need for **strong authentication**, one of them (#p3) mentioning the need of a **common identification scheme** which can be trusted by all parties, because part of the authentication process will occur beyond the supervision of the bank.
- Interviewees #p2, p4, and p5 had the same view that **response to threats** in general is a challenge because of several intertwining factors that include poor data analysis and the lack of common, interoperable methodologies. In addition, a considerable obstacle is that the security levels and prerequisites across the EU differ a great deal from each other. A final challenge is to be able to strike **balanced trade-offs between user privacy and cybersecurity** in the EU.

#### 4.1.2. Requirements

Fundamental capabilities will be needed to address the challenges described above, for instance **a strong ecosystem of exchange of critical information to fight against bank fraud**, the establishment of a **maturity model of business security**, or yet a **transversal digital identity platform** for banking players, focused on the end-user. Several specific key requirements that will contribute to creating such capabilities were stated and/or elicited from the interviews:

- Interviewees #p1 and p2 judged that **infrastructure cybersecurity** was especially important as a requirement, including cloud-computing protection, sound encryption techniques and the maintenance of secure credentials. At the EU level, best practices to security governance must be shared.
- Interviewee #p3 favoured the approach where authentication flows would be user-centric decoupled, in such a way that the user should not need to authenticate towards each and every bank to fetch and exchange data, but rather through a **federated authentication solution**, e.g. using eIDAS. Such a strong authentication should require a commonly recognised token scheme which is trusted by the different parties.
- Interviewee #p4 proposed an approach with which risks and awareness would be specified and addressed depending on solutions and end-users. Also proposed was the homologation and **certification of cybersecurity experts** at the EU level.
- Interviewee #p5 had a more general, higher-level view on requirements, citing **safe user experience, customers' trust**, and **high availability** of the Open Banking services.

The requirements above were expressed from the perspective of production and operational environments in European Open Banking, but they are shared by stakeholders in the financial sector worldwide. For instance, authentication and identification issues are prominent in emerging countries [22], while privacy concerns permeate the fintech sector, as shown in [23]. Usability issues of secure 2-factor authentication (2FA) schemes have been researched especially for e-banking applications [24,25] or other contexts [26–28], while other usability studies show that useable 2FA solutions exist [29,30]. Meanwhile, the scientific community is exploring possible technological, procedural, and social solutions to meet such needs. Solutions include those described in Section 4.3, below, as well as proposals for maturity and cyber-resilience models [22,31].

Training and education aspects, including awareness-raising and the certifications of experts, also rank high on the requirements list and are the focus of many organisations, such as Cybersecurityguide, which addresses the USA market,[12] and the European Commission's JRC, for Europe.[13]

### 4.2. Supply chain

Supply Chain is today considered one of the oldest and most widespread sectors in our society, which has gone through four different industrial generations to reach Industry 4.0 [32]. This new generation aims to create dynamic environments, converging the new Information Technologies (ITs) with the existing Operational Technologies (OTs), allowing to decentralise the entire value chain and automate operational tasks [33,34].

According to Gartner's 2021 Supply Chain Predictions report [35], 72% of organisations understand that new technologies are a source of opportunities for business. This makes applications built under the umbrella of Industry 4.0, such as supply chain scenarios, aim to envision a competitive and robust market, producing and distributing services and products according to actual demand. For this reason, it is also forecasted that by 2025 [35], more than 50% of supply chain organisations will comprise a significant technological deployment, investing in applications with support in Distributed Ledger Technologies (DLT), AI, and Big Data together with advanced analytics tools, among others [36].

#### 4.2.1. Key problems and challenges

The conducted interviews (17) in the area of supply chain identified the following problems and challenges in regard to needs specified below:

- **Dynamic risk assessment** (#p7 and p9). The number of risks and threats increases with technological convergence in these types of industrial ecosystems, and especially in the operational flows of a supply chain as explicitly stated by [37]. In [36], Vikas et al. also emphasise that the vast majority of organisations struggle with supply chain risk management, especially in relation to third-parties and security breaches. Interestingly, this vision, which is part of the literature, is in line with the interviewees #p7 and p9. Both interviewees remark on the importance of the suppliers in this kind of vertical, in which suppliers should be based on dynamic and systematic security-oriented approaches to risks and business (#p7); and in this way, guarantee a major control over their own ecosystem.
- **Protection at all levels and authentication** (#p6–8, p10, p13, p15, p17, p18, p20–21). The new technological trends in industry and the participation of multiple stakeholders in industrial ecosystems (such as customers) force us to consider new security challenges to protect devices, their communications and systems. For example, at the hardware level, it is fundamental to protect intelligence and the edge processing of devices (as mentioned by #p6), their connections and messaging control, as well as data storage considering the use of the new technologies (e.g., cloud as mentioned by #p8).
  Regarding authentication, identity protection and access to critical devices are also essential. In this case, authentication must be subject to cryptography-based advanced methods to ensure access control to devices and the protection of identities. This challenge is in line with [36,38,39] of the literature. The authors point out how authentication must be applied throughout the entire value chain, and, especially, in heterogeneous and complex scenarios, where it is necessary to consider the technology PUF (Physical Unclonable Functions) [36] and the capacities of the RFID (Radio-frequency identification) technology [38,39].

[12] https://cybersecurityguide.org/programs/cybersecurity-certifications/.
[13] https://cybersecurity-atlas.ec.europa.eu/cybersecurity-taxonomy.

- **Dynamic event management, prevention and detection** (#p11). Currently, the complexity of the new industrial ecosystems is not helping in the accurate management of events. Any supply chain must be able to manage events dynamically and accurately, and detect and prevent anomalous states in optimal times taking into account the current recommendations and good practices, such as the NIST (National Institute of Standards and Technology) Special Publication (SP) 800-161 [40]. For this reason, the interviewee #p11 supports the idea of developing advanced and lightweight detection and prevention mechanisms in field devices. So far, some related advanced intrusion detection approaches have already been proposed in the literature such as [41,42]; both focused on complex and critical verticals.
- **Assurance measures** through verification and compliance with regulation frameworks (#p6–8, p13, p17, p19 and p21). Supply chain operations are critical by themselves, and they should comply with all the processes and regulations required for their proper performance and security.
- **Standardisation and certification** (#p8-9, p14, p17–18 and p20). There are not enough standardisation and certification mechanisms in these types of critical infrastructures; and it is still necessary to harmonise approaches toward cybersecurity with cooperation across Europe. Note that the interviews #p8–9, p14, p17–18 emphasised in certification (as also addressed by the ISO 28000 standard [43]), whereas that #p14 and #p20 mentioned the importance of the standardisation; even if some standards are available [43].
- **Trustworthiness of operations and services, and resilience** (#p8, p12, p14, p20). It is essential, in any critical infrastructure of this type, to ensure that all elements are permanently connected. All elements in the value chain and their connections must be safe to preserve the integrity of the product or the service, and this procedure can also comprise the need to preserve confidentiality and integrity of industrial data in hostile environments under sophisticated cyber-attacks. An example of potential attacks in Industry 4.0 can be found in [44].
- **Operational performance** and establish measures that help control the complexity of the system (#p6 and p10). The implicit complexities of the new IT-OT environments and the need to incorporate security measures add new operational challenges related to availability. Thus, any approach proposed must be optimised to ensure the availability of processes, resources and data streams when they are demanded. This feature is in line with the work [45]. The authors characterise how additional complexities may have a negative and direct effect on manufacturing plant performance.
- **Technological and security culture** (#p7, p10, p12, p14, p16, p18, p20, p21). There exists a special lack of knowledge, education and training of the appropriate use of the current technologies and the current policies and standards. Note that this challenge is also contemplated within the literature. For example, the NIST SP 800-61 [40] includes it as part of its recommendation.

#### 4.2.2. Requirements

Key requirements elicited from the interviews related to the area of supply chain are summarised as follows:

- **Traceability, procurement and accountability** (#p12, p19–20). Specifically, these requirements are related to the need to explain the origin of the components and the trust level, the ownership of elements/parts of the supply chain, and the active management of its stakeholders. For this reason, transparency mechanisms such as Blockchain could be key to ensure traceability of actions and states within a particular ecosystem and guarantee accountability capacities. This feature is widely considered by #p12, p19–20, but also by the literature [36,46,47].
- **Governance and assurance** (#p6, p8, p21). Apart from applying regulations for safety (as specified by #p8 and #p21), it is also necessary (i) to consider the implementation of effective security metrics and controls (also addressed in the literature by [48]) to avoid exposing the underlying system and its own processes to vulnerabilities; and (ii) to be capable of applying policies according to security requirements and standards. With respect to assurance, it is fundamental to guarantee penetration testing in order to discover vulnerabilities as stated by #p22, and provide methods and tools that work at an interchangeable format across Europe.
- **Standardisation and certification** (#p6–7, p14 and p20). The development and enforcement of regulatory frameworks based on standards (#p20) and certification tools (#p8–9 and p14) is necessary.
- Resilience through **prevention and reaction** (#p11, p15–16); all of them should be working in optimal times. However, prevention and detection were emphasised by #p11, whereas the need to manage incidents was contemplated by #p16.
- **Security services by default** (#p6, p10, p12–13, p15, p18–20). If (i) availability, integrity and confidentiality, (ii) secure access, and (iii) detection of unforeseen events or anomalous states are required in supply chain scenarios as stated in previous section, then determined security services should be implemented by default. These services should, for example, be associated with authentication or authorisation mechanisms (#p10, p15, p18–21), or encryption primitives (#p6, p12–13, p19).
- Security awareness through **education and training** (#p7, p10, p12, p14, p16, p18 and p21). Most of the interviewees (especially #p7, p14, p21) have reflected on the lack of education about security issues and new IT solutions. This means that it is still required to plan regular training (e.g., in threat hunting as stated by #p16, or administration issues as mentioned by #p10) to be aware of the new conditions that the new industrial ecosystem brings to the supply chain (#p7 and p21).

Many of the problems and requirements noted by the interviewees are also considered by international organisations such as NIST [36], ENISA [49] or ECSO (European Cybersecurity Organisation) [50]. All of them emphasise how the entire supply chain remains a threat target, underlining the need to create trustworthy supply chains that promote robust markets and guarantee full end-user trust. However, this weakness also highlights that the advances established in the current literature [36,51] are not sufficient to meet the emerging needs of Industry 4.0 (e.g., autonomy, decentralisation, synchronisation, intelligence, mobility, interconnection, etc.) and its own supply chain. For this reason, we have reviewed the new priorities according to experts in this field, so as to list the most prioritised security requirements and the main challenges that may impact on the industry of the future and its supply chain, such as certification, training, education and resilience.

### 4.3. Privacy-preserving identity management

The objective of Privacy-Preserving Identity Management is to develop a highly efficient and scalable identity management solution supporting security, privacy and usability guarantees to all parties. Through the use of privacy-preserving crypto solutions, users should be empowered to manage their personal data in a trustworthy and privacy-preserving manner when interacting with service providers. For this, the inclusion of (i) security and privacy recommendations, (ii) usability requirements, (iii) legal and regulatory requirements or (iv) operational requirements have been identified as paramount [52].

#### 4.3.1. Key problems and challenges

Main problems and challenges identified from the 10 interviews that we conducted for this sector can be summarised as follows:

- **Combining privacy, usability and trust**. Interviewees (#p22, p23, p24, p26) emphasised the challenge to **construct IDM in a strong privacy-preserving and easy to use manner**. The core challenge is to develop IDM solutions that satisfy all the following three requirements at the same time: (1) strong privacy protection in terms of data minimisation, (2) no single point of failure or trust, (3) usability.
  Most privacy-preserving IDM technologies that already exist satisfy at most two out of the three requirements above. For instance, current privacy-preserving IDM solutions based on attribute-based credential (ABC) protocols, such as idemix [53], researched and developed by projects such as PrimeLife [54] and ABC4Trust [55], provide strong privacy in terms of data minimisation through unlinkability and selective disclosure options for the users. However, they take a decentralised approach for achieving user control, which requires users to obtain and manage credentials and encryption keys. Such actions are often not easy to understand or to perform by the users, and the crypto operations involved also raise performance issues, for instance if run on smart cards. Moreover, with attribute-based credential protocols the user still needs to trust third parties, such as the revocation agent, which is a privacy trade-off.
- **Dual knowledge gap:** Interviewees (#p22, p23, p24) stated a knowledge gap, especially in terms of a lack of security specialists available with dual understanding and knowledge of technologies and policies.
- **Lack of useable key management solutions**. It was also especially emphasised that useable key management solutions allowing key holders to be securely authenticated are lacking (#p22). This is especially a problem for user-centric privacy-preserving identity management solutions for which users have to engage with cryptographic protocols, such as ABC protocols, for proving properties.

A recent usability study [56] identified usability-security-trust trade-offs for key management solutions for secure email that are related to these challenges and observed that many users would in the end trade strong security in favour of enhanced usability. Alpár et al. [57] discuss related security, privacy, trust and usability challenges of IDM and further explore problems concerning ill-understood trust assumptions and challenges of managing complex situations of changing identities or managing complex transactions requiring multiple credentials. The challenge of combining privacy, usability and trust is currently approached by the OLYMPUS project on "Oblivious Identity Management and User-friendly services, based on the concept of a distributed oblivious identity management, where the role of the identity provider is split over multiple authorities [58]. OLYMPUS targets to adhere to existing identity management frameworks including idemix [53], SAML, OpenID connect, and does not require users to store long-term credentials.

#### 4.3.2. Requirements

The following key requirements were elicited from the interviews:

- There is a need to **simplify privacy-preserving IDM**, instead of trying to fit all the features into the same system. In particular, many existing IDM solutions in practice lack strong and end-to-end authentication, which should be a main goal. Therefore, the suggestion is to step back from theory and the goal of "maximum privacy" and rather address practical "good-enough" privacy requirements that make suitable trade-offs with usability, performance and costs, which are thus also economically viable. Practical examples of good privacy-usability-performance-costs trade-off solutions are Cloudflare [59], Privacy Pass [60] or CREDENTIAL [61,62], which are however not much used in practice and should be further promoted and deployed (#p23)
- **Awareness needs to be raised**, in particular, of non-technical decision makers, of what online privacy risks are, and what technical solutions exist (#p22, p23, p24, p25, p26, p30). There is especially the need for awareness and education in privacy-preserving cryptography, which is often counter-intuitive and thus hard to believe and hard to understand. This problem was also earlier pointed out by [63,64]. Especially managers and policy makers need to understand better what is technically possible with "crypto-magic" (#p22). Security awareness and culture need to be raised also in organisations in order to increase security awareness and trust in IDM technologies (#p22, p23, p24). Currently, a good security mindset does not exist in all sectors. While for certain areas in the banking sector there is a high level of security awareness, it is much lower in production environments, even though cybersecurity is equally important there (#p24). Also, awareness about the importance of multi-factor authentication as a basic secure building block for IDM needs to be raised for both users and companies (#p26, p29).
- **Secure and re-useable implementations of crypto for privacy-preserving technologies** – Privacy-preserving cryptographic systems are mostly designed by mathematicians, but are often not well implemented by software developers. In particular, vulnerabilities of devices need to be considered as well. Reusable Open Source implementations of privacy-enhancing technologies (PETs) and privacy-preserving crypto blocks are needed for developers, which can be easily adopted in current identity management systems (#p23). In particular, there is also a need to develop post-quantum resistant technologies (#p26, p30).
- Research and **guidelines are needed on proper implementations of the EU General Data Protection Regulation (GDPR)** [2] and its requirement for Data Protection by Design and Default (Art. 25 GDPR), as there are different degrees of data minimisation and it is hard to judge for practitioners what "appropriate technical and organisational measures" for implementing data minimisation are.
- **Stronger enforcement of the GDPR** for increasing citizens' control over their data as well as the need to penalise major IT companies who breach the GDPR and users' rights and mis-use their personal information were suggested by interviewees #p25, p26, p27 and p31.
- **Useable solutions** that can help users to remember and **handle cryptographic keys**, including secure backup and recovery keys need to be researched and developed (#p22). In general, there is a need to improve user experience for PETs (#p25, p27, p28, p31).

### 4.4. Incident reporting

The incident reporting sector has the objective to allow organisations or their entities to collaboratively report security incidents detected in a faster and legally compliant way, in accordance with the different procedures and methods specified by applicable regulatory bodies, such as PSD2 and the European Central Bank (ECB) Cyber Incident Reporting Framework [65]. The environment of the European digital single market and its transformation into a set of highly interconnected systems highlight the potential magnitude of the impact of cybersecurity incidents, where cyber-risks cross not only national borders, but also sector borders, resulting in potentially dramatic systemic risks [66]. Therefore, it is important to adopt a holistic vision of incident reporting and to promote a collaborative approach in order to improve, in particular, the cyber-resilience of the European cyberspace.

#### 4.4.1. Key problems and challenges

The key challenges stated in the 11 interviews can be divided into the following four categories:

- **Lack of ability to prevent and detect incidents in the first place.** Interviewee #p32 specifically identified the lack of criteria and metrics for good security architectures and security solutions, as well as for methods how to achieve them. Better mechanisms to hide and/or manage complexity were also cited by #p32, while #p36 found that Incident Response cycles lacked flexibility. Interviewee #p40 mentioned that not all systems necessarily generate event logs, which is an obstacle for the discovery of incidents.
- **Low technical capabilities in response to cybersecurity incidents.** Interviewee #p34 judged that key challenges in this area stem from the lack of trust, good analytics, and security in the exchange of data. Interviewee #p42 concurred in that even AI (Artificial Intelligence) solutions cannot yet be certified for their correctness and efficiency, and that there is a lack of access to verified and trustful Threat Intelligence information.
  For interviewee #p39, a major challenge is the lack of investment in SIEM (Security Information and Event Management) capabilities.
- **Lack of harmonised procedures for cybersecurity incident reporting across the EU.**
  Interviewee #p41 said that the risk of reputation loss tends to stop organisations from reporting the incidents they suffer. In addition, the multiplicity of authorities to which to report incidents (e.g., according to the NIS-Directive, PSD2 and GDPR) renders the reporting process very complex, with several to many authorities requiring different kinds of information (see, for instance also [67–70]).
- **Trained staff to manage security incidents, from detection to reporting.** Interviewees #p32, p33, p36, and p39 mentioned that the availability of capable human resources is a major blocking factor for efficient incident reporting. In particular, there is a knowledge gap, since there are only few security specialists available with dual understanding and knowledge of both technologies and policies. At a very basic level, even making employees understand what is a security incident and what is not (e.g. spam) is considered a challenge. It is thus very difficult to find competent and qualified personnel to join cybersecurity teams.

#### 4.4.2. Requirements

The requirements identified in the interviews aim to develop the coordination, financing, and support of efforts to accelerate the emergence of an advanced, innovative, dynamic, and integrated cybersecurity ecosystem that ensure the dissemination of basic and advanced skills and solutions to all economic sectors, critical and non-critical, and to all stakeholders. Unsurprisingly, such requirements mainly cover the problems and challenges that were elicited. Training, for instance, is a transversal issue considered as a basic requirement, and is not detailed below. On the other hand, many respondents want to avoid having incidents to report, by means of better cybersecurity options in terms of protection of the ICT systems involved.

A compilation of the responses provided is given in the following, grouped into three main requirement areas.

- **Controls and Reporting Techniques to avoid incidents in the first place.**
  Interviewee #p34 proposed to have far more effective security controls in practice, which include, according to interviewee #p38, the assurance that all connected elements are safe and all systems and devices to be deployed (in cities, cars, etc.) are accredited. Interviewee #p35 included the need for far-reaching protection from intrusion by state and non-state actors, while interviewee #p36 suggested the establishment of threat-hunting teams, focused on threat hunting for the rapid and proactive identification of new threats.
  Interviewee #p37 would like to have means to use Security Incident reporting to help in vulnerability assessment, and interviewee #p33 required security protection to be mass produced. The same interviewee thinks that security by design and privacy by design would help bringing a better security culture to the engineering of products and services. We note that this area is being researched and recommendations for aspects connected to vulnerabilities disclosure already exist [71], even though they still have to be implemented widely in Europe.
- **Detection of and response to incidents.** There were many requirements covering this topic, as eight of the interviewees mentioned something related to it, including specific training for technicians so that they learn what to do in case of security incidents, by interviewee #p39.
  Interviewees #p34, p36, and p42 want automated analysis tools that can demonstrate their level of efficiency. Moreover, in order to be able to build meaningful reports, interviewees #p33, p38, p39, and p40 suggested the development of appropriate software for log correlation, event traceability, and even for dealing with the identities of Internet of Things (IoT) components, based on encrypted access to assure the identity of the users and protect access to the devices.
  Interviewees #p36 and p41 proposed threat-intelligence and emergency-response teams to work in the incident cycle, including a centralised European Computer Emergency Response Team (CERT), open for all, with open-data API at least for Traffic Light Protocol (TLP)-Green data-sharing. In the area of data-sharing, interviewees #p35, p40, and p42 want means for simple and trustful data-sharing, including the ability to safeguard sensitive information, by securing logs against attacks, deletion, or modification, which is essential to facilitate information-sharing by security actors.
- **Harmonising procedures for cybersecurity incident reporting across the EU.**
  This topic was also very prominent, with related requirements being exposed by six interviewees. The main idea is to have harmonised procedures for cybersecurity incident reporting, for instance with the establishment of a European referential of incident typology or the mandatory homogeneity of event logs, as proposed by interviewees #p40 and p41.
  According to interviewee #p32, such harmonised procedures should certainly bridge the gap between policy and technology, including the possibility to have a direct contact with customers in case of personal data leak, as suggested by Interviewee #p42, in a way that makes incident reporting compatible with the GDPR, as proposed by Interviewee #p37.
  More closely to the operations, interviewee #p34 stated that automated trust-building technologies and new certification models are particularly needed, while interviewee #p37 put priority on linking the Security Incident reporting with cybersecurity awareness tools and on producing a Security Incident reporting repository and registry.
  Finally, interviewee #p34 remarked that, once the report itself must be sent, common procedures should ensure that the reported data is properly protected.

These needs are shared not only by cybersecurity managers across industry sectors, but also by operational actors, like CSIRTs, as shown in [72,73]. Both from the requirements list above and from the scientific literature, it appears that most of the possible solutions belong in the organisational domain, including education, training, ontologies and taxonomies, maturity models, standards, and procedures [74–76].

On the other hand, a great deal of hope is put on solutions based on Artificial Intelligence, which could help accelerate the detection of security incidents with the use of Machine Learning techniques [77]. However, as pointed out in the interviews, existing operational solutions are yet to be certified for either correctness or efficiency.

### 4.5. Maritime transport

The maritime transport ecosystem provides a collaborative and complex process that involves domestic and international transportation, communications and information technology, warehouse management, order and inventory control, materials handling and import/export facilitation, among other things. The Maritime Transport system involves several different actors, in a multitude of countries spread all over the globe. Thus, the attack surface (i) is large, (ii) will probably be getting larger, and (iii) cannot be controlled or protected by a single entity. To make matters worse, the nature of this sector gives rise to *hybrid* attacks where cyberattacks are combined with physical access (such as piracy) to amplify physical attacks or to launch attacks that are larger than previously possible [78].

#### 4.5.1. Key problems and challenges

The following key problems were stated in 4 interviews that we conducted:

- **Lack of understanding.** Interviewees (#p43, p45, p46) emphasised that the threats in this area should be better understood. While one of them (#p45) focused on the dangers of the emergent IoT threats, the others took a broader perspective and suggested the need to understand threats possibly through a continuously evolving **threat landscaping** process.
  Overviews to landscapes of cybersecurity threats in maritime transport that could contribute to that end were also presented recently by the literature [79,80].
  One interviewee even suggested to broaden the focus to include not only maritime threats, but threats that apply to all other kinds of transport.
- **Lack of cybersecurity culture.** Interviewee #p44 pinpointed that cybersecurity culture should be created within the maritime operations. He suggested that some ports and maritime providers do not have a mature cybersecurity culture. Indeed, they do not adopt good Information and Communication (ICT) supply chain security, they are not aware of emerging cybersecurity threats, and are not prepared for catastrophic cybersecurity attacks.
  It seems however that the problem of cybersecurity culture is much deeper: as pointed out by the literature, it is not that we do not have a solution to it - we do not even have a good definition for it [81,82].
- **Lack of standards and methodologies.** Interviewee #p44 also mentioned that there is a lack of standards and methodologies, which can help in the assessment of risks and their cascading effects, should be adopted.

#### 4.5.2. Requirements

The following key requirements were stated in and/or elicited from the interviews:

- All interviewees suggested that we need to focus on **education and training**. They underlined the need for training systems, curricula, and simulation environments such as war games supported by tools to test scenarios and conflict situations to support the decision-making process in the maritime sector. It is obvious that untrained personnel can easily be the weakest link in the cybersecurity chain.
- Interviewees #p44 and p46 called for **novel governance models**. In particular, #p44 called for collaboration between public and private entities to develop centres for cybersecurity incident handling. Such centres may also provide education and training (see above) and close the cyber skills gap. Such training may be provided through exercises (cyber ranges) that involved realistic evidence-based experiments. Such cyberranges may also involve the NATO and ENISA.
- Interviewee #p44 calls for a close **collaboration between civilian and military maritime security teams**. Such collaboration may include the creation of a common maritime security centre, and/or common certification efforts.
- Finally all interviewees call for more work on basic security technologies: cyberattack detection, encryption of communications, software security, and so on.

### 4.6. Medical data exchange

Processing information efficiently is vital to healthcare providers in order to address patient care, advance the operational process and meet the changing regulatory mandates. The Medical Data Exchange sector has the objective to enable a secure and trustworthy exchange of sensitive data between several players who have different aims and claims, which is in line with applicable legislation and the strategic policy framework (the EU General Data Protection Regulation (GDPR) [2], the EU Network and Information Security (NIS) Directive [3], the EU Commission's blueprint for rapid and coordinated incident response [83], and recommendations on security and privacy from the European Network and Security Agency (ENISA) (e.g., [84,85]), etc.).

#### 4.6.1. Key problems and challenges

The conducted interviews (9) in the area of medical data exchange identified the following key problems and challenges that should be addressed in the future:

- **Data processing in compliance with the GDPR.** Medical data are as special categories of data especially protected by the GDPR (Art 9). Today, many organisations are however not well prepared to collect, process and handle medical data in a GDPR compliant way. For instance, the data protection by design principle of the GDPR (Art. 25) could be met if the data were anonymised or pseudonymised when stored in the cloud, but it is uncertain for the companies how to apply data privacy technologies to achieve secure anonymisation or pseudonymisation (#p51, p49). Moreover, there are also the challenges for technical experts to understand and translate the GDPR rules for obtaining consent in a useable and lawful manner (#p48, p49).
- **Lack of awareness, lack of trust.** A knowledge gap (#p48, p50) in terms of security on the management level along with the lack of security awareness (#p52, p53) about risks related to medical data and medical infrastructures was also highlighted in the interviews. Many incidents in which patient information has been mis-handled have been reported in the media (such as the recent data breach with the 1177 eHealth service in Sweden[14]) which has challenged trust in eHealth systems.
  Coventry et al. [86] discuss similar cybersecurity challenges in healthcare and point out that the ongoing publicity associated with large security breaches may compromise patient trust which could in turn result in reduced willingness to share data.
- **Technical security measures are not up-to-date.** A lack of up-to-date security measures in relation to the storage and overall handling of health data may result in incidents proliferation (#p51, p48). For instance, if a large amount of data (e.g., genetic data) need to be stored, organisations may need to outsource the storage to the cloud. However, clear or appropriate security measures for secure data transfer to the cloud are often missing for organisations in practice. Furthermore, the interviewees (#p52, p51, p55) point out the security challenges of IoT and medical devices generating the data.

[14] For more information about the 1177 data breach, see for instance: https://www.bbc.com/news/technology-47292887.

- **Lack of rules for medical data exchange across countries.** According to interviewee #p49, there is a lack of standardised rules for medical data exchange between the national contact points in different countries. Companies located in different countries have different rules and regulations on how medical data should be exchanged. This shortcoming hinders the efficient and interoperable cross-border health data exchange, which clearly identifies the need for enabling a trustworthy exchange of sensitive data between several players within the European Union. This problem and other technical, ethical and legal challenges were also researched by the EU project KONFIDO [87], which presents the current landscape for evolving eHealth infrastructures for cross-border medical data exchange in Europe.
- **Secure and useable authentication.** Three interviewees (#p47, p52, p55) highlight the challenge to implement secure and useable authentication. While smart cards and two-factor authentication have been implemented in some health care systems, many password-based systems are still in use. Because today's methods for authentication are not fast and easy enough, the healthcare personnel often perceive it as cumbersome and find ways to avoid re-authentication, for instance by sharing login, not logging out, etc (#p47). The GDPR demands the implementation of appropriate security measures for protecting personal data, and is thus implicitly requiring multi-factor authentication for medical data and other special categories of data that are *per se* regarded as very sensitive. Multi-factor authentication is however difficult to implement in practice in health care environments and it is not even supported by some vendors of electronic health care solutions.
- Furthermore, today the healthcare systems face **difficulties to implement access control, logging and IDS** (#p47, p55). Since many organisations still have an access model where all personnel can access all patients' data, insider attacks violating the least privilege principle in health care are difficult to detect, e.g. if a doctor from a department other than the one treating the patient was allowed to look into a patient file or not. There is a trade-off between patient safety and privacy, it is still a challenge to define and enforce data access by medical personnel following the least privilege principle and to analyse logs automatically. Overcoming these barriers will require a more process-oriented workflow which would help to identify departments, personnel roles and patient groups to be used for modelling access control (#p47).

#### 4.6.2. Requirements

Key requirements elicited from the interviews related to medical data exchange are summarised as follows:

- There is a need for **appropriate technical security measures if a large amount of data needs to be stored in the cloud** (#p49, p55, p51). There is uncertainty for companies what appropriate/adequate data privacy technologies are required in different contexts (e.g., how data should be anonymised/ pseudonymised if outsourced to the cloud). Therefore, the suggestion is to focus on building architectures for outsourcing sensitive data in a secure way while preserving data subjects' privacy in compliance with GDPR rules and guidelines. There is especially the need to ensure the confidentiality and integrity of sensitive health data by using state-of-the-art technologies such as homomorphic encryption and a dedicated blockchain/ledger which would provide a patient-centred solution for increasing transparency of data processing (#p55).

  Blockchain based approaches providing data provenance, auditability, and control over medical data exchanges between different entities, as suggested by #p55, were recently also proposed and presented by [88,89].

  The requirement for appropriate cloud security measures is in line with the "Schrems II" decision of the Court of Justice of the European Union (CJEU) from 16 July 2020. The CJEU decision requires that standard contractual clauses as a legal basis for the use of non-European cloud servers need to be complemented with appropriate safeguards to individuals' personal data in accordance with the GDPR. On July 24, 2020, the European Data Protection Board (EDPB), issued guidance on and examples of such measures [90], such as securely pseudomymised data, which would according to Art. 4 (5) also include homomorphically encrypted data.
- **Privacy and security awareness needs to be raised** especially in respect to technical users for understanding legal rules (e.g., understanding how to enforce the consent in an easy, legally compliant way) (#p49). At the same time, non-technical users should also understand the risks of invading the patients' privacy and the basic threats of data breaches (#p52, p53).
- Nearly all the interviewees highlight the need of **increasing security competence** in the form of education and training at all levels (#p47, p50, p51, p52, p53, p54), in particular at the management level (#p48). There is also the need to improve the competence of vendors and developers in cybersecurity, secure coding, privacy by design and privacy by default.
- **Secure and easy-to-use authentication and authorisation** systems. There is the need to deploy better solutions for useable multi-factor authentications, single-sign on (SSO), Intrusion Detection Systems (IDS), role/context-based access control in healthcare (#p47, p48, p49, p52, p54, p55). Moreover, the development of crypto solutions for allowing the analyses on encrypted data on rest and data in transfer is needed (#p51, p48).
- **More regulations from the government**. While implementing requirements from the NIS Directive in an appropriate manner would help a great deal, there is a need for more regulations from the government in health care (#p48, p51, p55). In particular, there is a need for standards, guidelines and frameworks for the exchange of medical data between cooperating companies that have different rules and regulations (#p49). In that regard, the GDPR is a good example of a regulation that puts more pressure on the health care sector to improve the security and privacy of health care systems.
- Research and **secure development process for both networks and systems**, based on Privacy by Design and Security by Design. More research is needed to understand why it is very difficult to implement cybersecurity in healthcare (#p48). However, the research should not only focus on the technology needed but also on the non-technical organisational security perspective (#p50, p54), in terms of the best protection doctrine given the resources and technology that are required and the resources (including what skills people need) and technology that are available and economically reasonable (#p50). In addition, a sustainable and systematic approach to cybersecurity as well as Information Security Management Systems need to be implemented in health care (#p48). Thus, it should be required to implement appropriate security controls, conduct evaluations, educate personnel and implement follow-up measures.

A recent preliminary Opinion 8/2020 on the European Health Data Space (EHDS) by the European Data Protection Supervisor from 17 November 2020 [91] is also like our interviewees emphasising the necessity for organisational and technical data protection safeguards to be defined at the outset of the creation of the EHDS for achieving GDPR compliance (and the CJEU Schrems II decision), highlighting especially the importance of the data subjects' right to data portability in this context. In addition, this opinion also points out the essential need for complementing guidelines for the ethical and responsible use of such data.

Related requirements and proposed solutions for GDPR-compliant medical data exchange approaches have also recently been discussed: For instance, Larrucea et al. [92] propose to integrate consent management and data hiding tools over a Healthcare Industry architecture reference model, while the CUREX project presents a privacy by design approach to a decentralised architecture GDPR-compliant medical data exchange enhanced by a private blockchain infrastructure for ensuring the data integrity and thus patient safety [93]. Jin et al. provide a survey on secure and privacy-preserving medical data sharing schemes with a focus on blockchain-based approaches [94].

### 4.7. Smart cities

Smart cities, through an interconnected network of sensors and actuators, have the opportunity to provide novel and useful services for their citizens. At the same time, the data collection done by all these sensors has the potential to invade privacy and to pose a serious security risk. Striking a balance between (i) providing useful services and (ii) protecting privacy is a challenging task that needs to be addressed.

#### 4.7.1. Key problems and challenges

The conducted interviews (8) in this area identified the following challenges:

- **Lack of clear procedures**. Interviewee #p57 suggested the need to have a clear procedure for data collection and management. Indeed, smart cities involve a wide variety of sensors and actuators, operated by different (usually private) organisations which may process (potentially personal) data of citizens. Having a clear process of who is accessing what seems to be of paramount importance. Otherwise, we will probably see data leaks which will eventually erode the trust of the citizens in the services offered by smart cities.
- **Complex authentication**. Both Interviewees #p56 and p57 mentioned the need for simple and trustworthy authentication. Interviewee #p57 focused on simple and secure authentication, while interviewee #p56 focused on the trust placed in the government for authentication. Providing a simple and trusted authentication mechanism seems to be the challenge here. Single-sign-on systems will probably be the most convenient for end users, but at the same time, they will be the hardest to implement in a heterogeneous environment.
- **Need to capitalise on sophisticated analytics**. Interviewee #p58 suggested the need for good analytics as this is one of the best ways to understand how a city actually works. Since a smart city involves the interplay of many actors, there is usually no single place that offers a global view of all operations. Analytics may help create this global view of the city's operations.
- **Lack of Privacy Enhancing Technologies**. Interviewees (#p60 and p63) proposed the need for privacy and possibly the use of PETs (Privacy Enhancing Technologies) that will protect the privacy of users contributing their data. When sharing personal data, privacy becomes of paramount importance and ensuring it cannot be done as an "afterthought".
- **The current mode of reactive operation is outdated**. Interviewee #p58 suggests that the mode of operation of current cities should change. Indeed, current cities today usually *react* to situations, especially in cases of emergency.
- **Lack of strong encryption**. Interviewees #p59 and p60 mention that several of the deployed devices have minimal security protocols and several of them do not employ end-to-end encryption. It seems that without encryption, it is extremely difficult to provide trust, authentication, and data provenance.
- **Fleet Management: updates and patching**. Interviewee #p62 pinpoints to the challenge of securely updating the devices with the most up-to-date patches. Indeed, although the deployed devices may initially be secure, they need to be frequently updated, especially since they will operate in an unfriendly, if not hostile, environment.

#### 4.7.2. Requirements

The following requirements were stated:

- **Trust**: Interviewees #p56, p57 and p59 underlined the necessity of trust: trust in the people to their government and in the digital services that they use; trust of the people in the system; trust in the mechanism that will share their data.
- **Proactive mode of operation**:Interviewee #p58 suggests that cities should transform their mode of operation and move from a *reactive* mode to a *proactive* mode. The availability of big data and data analytics performed on them can facilitate this transformation. This may profoundly change the way cities operate and the kinds of services enjoyed by their citizens.
- **User-centric control**. Interviewees #p56 and p60 suggested that individuals should have control over the use and sharing of their data. Data should be open and shared, but under the control of individuals. This is an obvious requirement that has recently found a significant legal support with the introduction of the General Data Protection Regulation (GDPR). Citizens now expect to be in control of their data. They may be willing to release (some of) their data, but they are not willing to release control.
- **Certification and Authenticity**. Interviewees #p61 and p63 underlined the importance of certification and authenticity. Indeed, data from the sensors should be authentic and cyberattackers should not be able to tamper with them.
- **Traceability - provenance**. Finally interviewees #p57, p60, and p61 proposed that data should be traceable to their original source for transparency and accountability. If data can be tampered with, then the results based on these data will not be trusted anymore.
- **Interoperability - Standardisation**. Interviewees #p59 and p63 mentioned the need for interoperability among different IoT devices; interoperability that can be achieved through the use of standardisation. Since all the sensors and actuators are manufactured by different companies in different countries, interoperability seems to be both a requirement and a challenge at the same time.

Requirements for privacy-enhancing technologies and user-centric privacy controls for smart cities are also discussed in [95]. Moreover, recent literature surveys on security and privacy challenges and requirements [96,97] are mostly in line with our findings, but also address more specific challenges such as Botnet activities in IoT-based smart cities, privacy issues of virtual reality and smart mobility. The surveys also discuss threats posed by AI including adversarial attacks on machine learning. Interestingly, even though data analytics for providing a global view of operations and for supporting proactive modes of operation was discussed in our interviews, security of machine learning and adversarial attacks (as e.g. presented in [98–100]) was not mentioned as one of the key challenges by the interviewees.

## 5. Discussion: Commonalities

This section illuminates the common points that have emerged in the analysis of at least two sectors. Such commonalities give a clear view on where to prioritise policy design that is meant to foster research on specific areas. In case further prioritisation would be needed, then a further study about the broader impact of each of these commonalities should be performed. As we have done in the previous section, we will group the commonalities in terms of key problems and challenges on the one hand, and requirements on the other.

### 5.1. Common key problems and challenges

- Building trust. Depending on the sector, the need for trust is conceived in different ways. Thus, in the case of smart cities, federation of trust is the challenge, building trust in other sectors or trusting the data holder. The establishment of trust is essential for information sharing in any sector, although for maritime transport and supply chain the achievement of trustworthiness is highlighted as especially relevant.
- Privacy and identity management. The challenge of privacy is manifold. Most of the sectors consider the achievement of privacy as a key challenge. Thus, for medical data exchange the main concern, apart from how data are treated, is the need to be compliant with the GDPR, whereas in the open banking case the stakeholders refer to confidentiality and proper identity management as a key point. In the smart cities use case the interviews also mention, related to privacy, how to define clear procedures which regulate who can access the data. Also, in this sense, for the privacy-preserving identity management, the highlighted challenge is the combination of some requirements: strong privacy, trustworthiness and usability.
- Secure and useable authentication. All the sectors consider the need for authentication as a challenge, closely related to identity management. Of special relevance is the difficulty to implement useable authentication, access control and logging in health care. The implementation of useable two-factors authentication implicitly required by the GDPR for accessing special categories of data is a special challenge in health care systems, for instance.
- Resilience. This challenge is especially important in sectors that are critical, particularly the maritime transport and the supply chain sectors. In these cases, building resilient systems becomes essential as a failure in any operation might lead to disastrous effects. In particular, the term resilience by design is considered as a key challenge. This is not surprising as resilience has been a flagship project for ENISA[15] as well as for several researchers [101–103].
- Threat landscape or detection of fraud. The first term is used in maritime transport and for open banking scenarios the latter, however, they refer to the same idea. In this sector, stakeholders highlight the need to consider hybrid attacks as specific for them. A related challenge is considered by the Supply Chain sector as event management, prevention and detection. In the same direction, the stakeholders for the Privacy-preserving Identity management sector highlight the need for more effective security controls that avoid them to be exposed to vulnerabilities. In the case of smart cities social engineering might be a source of attacks for smart devices.
- Training and cybersecurity culture. This is horizontal challenge for all the sectors. In general, all the stakeholders agree on the lack of cybersecurity professionals to be hired by companies. In the same direction for some sectors, such as the maritime transport one, this challenge is addressed as security culture in new cybersecurity threats that might arise. Underlining the importance of this direction, ENISA has created an entirely separate activity on cyber exercises[16] that includes studies and training.
- Standardisation and certification. Supply chain and maritime, medical data exchange need standardisation of methodologies. Certification for cloud providers is also needed.

[15] https://resilience.enisa.europa.eu/.
[16] https://www.enisa.europa.eu/topics/cyber-exercises.

### 5.2. Common requirements

By analysing the requirements specified for each of the sectors in Section 4, we can observe that some of them are common to all or most of them.

- Education and training. This is a requirement that has been considered as essential by all the stakeholders enquired for all the sectors. Then, for each of the sectors there are some specific professional profiles with specific knowledge that are needed. Thus, for instance, in the privacy-preserving identity management or secure medical data exchange sectors the required professionals should have specific knowledge on how to deal with the requirements of the GDPR.
- Raising cybersecurity awareness. This is slightly related to the previous one, not only in terms of education but in terms of making non-technical users aware of the cybersecurity risks that they might face in the respective sectors. It was especially mentioned as a requirement for the supply chain, privacy-preserving identity management and medical data exchange sectors, while in the open banking sector cybersecurity awareness seems to exist to a higher degree.
- Certification and standardisation. The need for having certified projects or using standard tools or technologies is considered by all the sectors. Thus, for example, the open banking sector mentions as a requirement the need for a transversal digital identity platform or the development of protocols using web standards. For medical data exchange it is mandatory that the cloud providers are certified in the field of health care.
- Resilience. All the sectors highlight the need for resilience as a requirement that must be met in all the cases. Thus, this requirement is especially important in supply chain, maritime transport and smart cities. In open banking, the requirement is considered as ‘smart decision-making’ systems that are able to adapt, and in smart cities the requirement is specified in terms of capacity of Small and Medium-Sized Enterprises (SMEs) to react to cyber-attacks as well as to specific resilient services and infrastructures.
- Security and privacy by design. Some sectors mention this requirement as such, however, it includes aspects such as verification and validation that are considered for all the sectors.
- Secure and privacy-compliant data exchange and information sharing. This requirement is closely related to security and privacy by design and might also involve some notions of trust. In addition, regulations that are GDPR compliant are related to the information sharing aspect.
- Regulations from the government side. All the sectors point out the need for governments to establish standards and guidelines that help implement the different regulations and rules across the EU. Of particular interest is the implementation of the GDPR in different countries.
- AI techniques. The benefits and need to use AI techniques in form of data analytics/machine learning for monitoring, detection and prevention of security threats were considered by the supply chain, smart cities and incident reporting sectors.

Interestingly, as also mentioned in Section 4, security of machine learning was, with some exceptions for the incident reporting sector, not emphasised and thus not considered by the interviewees as one of the key challenges. The reason for this may be that in the supply chain and smart city sectors, techniques based on machine learning were rather suggested for improving security monitoring, detection and prevention solutions by our interviewed stakeholders, but these techniques were however not in use yet at their organisations. However, recent research that found that industry practitioners are not equipped yet to protect, detect and respond to attacks on their machine learning systems [104] demonstrates that this challenge needs to be considered as very important as well.

**Table 2**
Research directions addressing common problems, challenges and requirements identified that are reflected by the CyberSec4Europe project's R&I roadmap [105].

| Research directions (identified by stakeholders) | Application areas that incorporate the research directions (taken from CyberSec4Europe R&I Roadmap) |
|---|---|
| Building trust | Medical data exchange |
| | Smart cities |
| Privacy and identity management | Privacy preserving identity management |
| | Medical data exchange |
| Secure and useable authentication | Open banking |
| | Privacy preserving identity management |
| Resilience | Maritime transport |
| | Smart cities |
| Standardisation and certification | Supply chain assurance |
| Security and privacy by design | Smart cities |
| Data exchange and information sharing | Medical data exchange |
| | Smart cities |
| Regulations from the government side | Medical data exchange |

### 5.3. Relation to CyberSec4Europe's Research & Innovation Roadmap

These common key problems, challenges and requirements identified for several demonstration use cases have already had an impact on the security research for the demonstration use cases of the CyberSec4Europe project.

In Table 2 we provide an overview of the common key problems, challenges, requirements that have been taken up as research directions (see first column of the table) by researchers of the CyberSec4Europe project. The second column shows the sectors where those dimensions were considered important in the Research & Innovation Roadmap of the project [105].

## 6. Conclusions

In this paper, we describe how we collected requirements for future cybersecurity research identified in several key sectors: Open Banking, Supply Chain, Privacy-preserving Identity Management, Security Incident Reporting, Maritime Transport, Medical Data Exchange, and Smart Cities. For all these security-critical sectors we interviewed key stakeholders that have direct and specific interests into, or interact with, such sector-specific ecosystems. The methodology that was used in the elicitation process, described in Section 3, facilitated the collection of important problems and challenges, especially for the mid- and long-term, in each of the sectors, also considering the European context in terms of recommendations (e.g., by ENISA), rules, and regulations (e.g., GDPR, NIS Directive, PSD2, eIDAS) that need to be met within the sectors. Such a landscape then induced requirements in capabilities, technologies, and other related measures that are going to be needed to address those problems and challenges in future. The main take-aways from the identification of the commonalities among the requirements elicited for the different sectors are as follows:

- Common challenges: Building trust, privacy and identity management, secure and useable authentication, resilience, threats identification and fraud detection, capacity building that include the development of a cybersecurity culture, and the establishment of standards and certification frameworks.
- Common requirements: Education, training, cybersecurity awareness campaigns, certified projects, widening the use of standard tools and technologies, resilient systems, security and privacy by design, and a secure and privacy-friendly environment where data are exchanged and information is shared in volumes much larger than today. The identified requirements are being taken up by the cybersecurity community all over Europe. In particular, universities create new education and training courses in the broader area of cybersecurity. Examples are presented by the cybersecurity education database created by ENISA,[17] and the cybersecurity training and education review created by the CyberSec4Europe project [106]
- Common technologies: Encryption and cryptography techniques, distributed ledger technologies, strong and useable authentication and authorisation mechanisms, trust management, tools based on Big Data, and Artificial Intelligence. These technologies have now formed the backbone of the CyberSec4Europe project [107].

In relation to these commonalities, it can be concluded that our stakeholders envision resilient systems, infrastructures, and societies as their common objective. It emerges from this task as a whole that their needs will only be fulfilled by an environment that wisely encompasses regulation, incentives, structural reorganisations, and capacity building, along with research and the deployment of new technologies.

While such common problems, challenges and requirements are tackled by the CyberSec4Europe project and other cybersecurity researchers and projects in Europe, there are still open problems and challenges that we have identified in Sections 4 and 5 , which require further mid and long-term research and innovation activities in Europe. Therefore, the results of this article can also help with identifying research and innovation directions beyond the work of the CyberSec4Europe project that will need further attention in Europe for the future.

## CRediT authorship contribution statement

**Simone Fischer-Hübner:** Conceptualization, Methodology, Investigation, Data curation, Writing - review & editing. **Cristina Alcaraz:** Investigation, Data curation, Writing. **Afonso Ferreira:** Conceptualization, Methodology, Investigation, Data curation, Writing - review & editing. **Carmen Fernandez-Gago:** Investigation, Data curation, Writing. **Javier Lopez:** Conceptualization, Methodology, Writing - review & editing. **Evangelos Markatos:** Conceptualization, Methodology, Investigation, Data curation, Writing - review & editing. **Lejla Islami:** Investigation, Data curation, Writing. **Mahdi Akil:** Investigation, Data curation, Writing.

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

[17] https://www.enisa.europa.eu/topics/cybersecurity-education/education-map.

## Acknowledgements

This work was supported by the CyberSec4Europe project funded by the European Commission's H2020 Programme under the Grant Agreement Number 830929. We want to thank all stakeholders that participated in the interviews.

## References

[1] European Commission. Joint communication to the European parliament and the council – the EU's cybersecurity strategy for the digital decade. 2020, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164, [Online; accessed 03-May-2021].

[2] Council of the European Union and European Parliament. 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). Off J Eur Union 2016;L119:1–88.

[3] Council of the European Union and European Parliament. Directive (EU) 2016/1148 of the European parliament and of the council of 6 July2016 concerning measures for a high common level of security of network and information systems across the union. 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC, [Online; accessed 02-November-2020].

[4] AEGIS. White paper on research and innovation in cybersecurity. aegis project. 2018, https://aegis-project.org/wp-content/uploads/2019/01/AEGIS-White-Paper-on-Research-and-Innovation-in-Cybersecurity.pdf, [Online; accessed 09-November-2020].

[5] Carmen Fernandez FM. D4.1 part II: Engineering secure future internet services: a research manifesto and agenda from the NESSoS community. NESSoS project; 2011, https://cordis.europa.eu/docs/projects/cnect/0/256980/080/deliverables/001-NESSoSD41PartIIRoadmap.pdf, [Online; accessed 09-November-2020].

[6] Amardeo Sarma AL. Strategic research agenda. Trust in Digital Life; 2012, https://trustindigitallife.eu/wp-content/uploads/2016/07/TDL-SRA-version-2.pdf, [Online; accessed 09-November-2020].

[7] President's Information Technology Advisory Committee. Cyber security: A crisis of prioritization. National Coordination Office for Information Technology Research and Development; 2005, https://www.nitrd.gov/pubs/pitac/pitac_report_cybersecurity_2005.pdf, [Online; accessed 08-November-2020].

[8] Markatos E, Balzarotti D, Almgren M, Athanasopoulos E, Bos H, Cavallaro L, et al. The red book. 2013.

[9] Bisson P, Martinelli F, Granadino R. Cybersecurity strategic research agenda-SRA. In: European network and information security (NIS) platform NISP-working group, Vol. 3. 2015, p. 1–201.

[10] ECSO. Strategic research and innovation agenda. 2017, https://www.ecs-org.eu/documents/publications/59e615c9dd8f1.pdf, [Online; accessed 04-November-2020].

[11] Anisetti M, Ardagna CA, Carminati B, Ferrari E, Perner CL. Requirements and challenges for secure and trustworthy uas collaboration. In: 2020 second IEEE international conference on trust, privacy and security in intelligent systems and applications (TPS-ISA). IEEE; 2020, p. 89–98.

[12] Kyrkou C, Papachristodoulou A, Kloukiniotis A, Papandreou A, Lalos A, Moustakas K, et al. Towards artificial-intelligence-based cybersecurity for robustifying automated driving systems against camera sensor attacks. In: 2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI). IEEE; 2020, p. 476–81.

[13] Mohamed N, Al-Jaroodi J, Jawhar I. Opportunities and challenges of data-driven cybersecurity for smart cities. In: 2020 IEEE systems security symposium (SSS). IEEE; 2020, p. 1–7.

[14] Vuksanović IP. Modeling an interdependent concept of cyber security in Croatian digital society. In: 2019 International conference on systems, signals and image processing (IWSSIP). IEEE; 2019, p. 145–50.

[15] Siddiqui Z, Zeeshan N. A survey on cybersecurity challenges and awareness for children of all ages. In: 2020 International conference on computing, electronics & communications engineering (ICCECE). IEEE; 2020, p. 131–6.

[16] ENISA. ENISA threat landscape. 2020, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends, [Online; accessed 08-November-2020].

[17] Aamodt M, Brecher E, Kutcher EJ, Bragger JD. Do structured interviews eliminate bias? A meta-analytic comparison of structured and unstructured interviews. In: Poster – Annual Meeting of the Society for Industrial-Organizational Psychology; 2026.

[18] Dana J, Dawes R, Peterson N. Belief in the unstructured interview: The persistence of an illusion. Judgm. Decis. Mak. 2013;8(5):512.

[19] Ferreira A. Deliverable D4.1: Requirements analysis from vertical stakeholders. CyberSec4Europe; 2020, https://cybersec4europe.eu/wp-content/uploads/2020/06/D4.1-Requirements-Analysis-from-Vertical-Stakeholders-WithAnnex-v14.0.pdf, [Online; accessed 08-November-2020].

[20] Council of the European Union and European Parliament. 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. 2016, https://eur-lex.europa.eu/eli/dir/2015/2366/oj, [Online; accessed 27-October-2020].

[21] Mani V. Cybersecurity and fintech at a crossroads. ISACA J 2019;2:1–7, https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2019/volume-1/cybersecurity-and-fintech-at-a-crossroads_joa_eng_0219.pdf, [Online; accessed 04-November-2020].

[22] Alghazo JM, Kazmi Z, Latif G. Cyber security analysis of internet banking in emerging countries: User and bank perspectives. In: 2017 4th IEEE international conference on engineering technologies and applied sciences (ICETAS). 2017, p. 1–6. http://dx.doi.org/10.1109/ICETAS.2017.8277910.

[23] Mehrban S, Nadeem MW, Hussain M, Ahmed MM, Hakeem O, Saqib S, et al. Towards secure fintech: A survey, taxonomy, and open research challenges. IEEE Access 2020;8:23391–406. http://dx.doi.org/10.1109/ACCESS.2020.2970430.

[24] Gunson N, Marshall D, Morton H, Jack M. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. Comput Secur 2011;30(4):208–20.

[25] Krol K, Philippou E, De Cristofaro E, Sasse MA. "They brought in the horrible key ring thing!" analysing the usability of two-factor authentication in UK online banking. 2015.

[26] Das S, Wang B, Camp LJ. MFA is a waste of time! understanding negative connotation towards MFA applications via user generated content. In: Proceedings of the thriteenth international symposium on human aspects of information security & assurance (HAISA 2019); 2019.

[27] Reynolds J, Samarin N, Barnes J, Judd T, Mason J, Bailey M, et al. Empirical Measurement of Systemic 2FA Usability. In: 29th USENIX security symposium (USENIX) security 20); 2020. p. 127–43.

[28] Dutson J, Allen D, Eggett D, Seamons K. Don't punish all of us: Measuring user attitudes about two-factor authentication. In: 2019 IEEE European symposium on security and privacy workshops (EuroS&PW). IEEE; 2019, p. 119–28.

[29] Reese K, Smith T, Dutson J, Armknecht J, Cameron J, Seamons K. A usability study of five two-factor authentication methods. In: Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019); 2019.

[30] De Cristofaro E, Du H, Freudiger J, Norcie G. A comparative usability study of two-factor authentication. 2013, ArXiv Preprint ArXiv:1309.5344.

[31] Dupont B. The cyber-resilience of financial institutions: significance and applicability. J Cybersecur 2019;5(1). http://dx.doi.org/10.1093/cybsec/tyz013, tyz013.

[32] Bakuei M, Flores R, Kropotov V, Yarochkin F. Securing smart factories in the era of industry 4.0. TREND Micro, research; 2019, https://documents.trendmicro.com/assets/white_papers/wp-threats-to-manufacturing-environments-in-the-era-of-industry-4.pdf, [Online; accessed 08-November-2020].

[33] Mantravadi S, Schnyder R, Møller C, Brunoe TD. Securing IT/OT links for low power IIoT devices: Design considerations for industry 4.0. IEEE Access 2020;8:200305–21.

[34] Ivanov D, Sethi S, Dolgui A, Sokolov B. A survey on control theory applications to operational systems, supply chain management, and industry 4.0. Annu Rev Control 2018;46:134–47.

[35] De Muynck B, Aimi G, Titze C, Stevens A, Klappich D. Predicts 2021: Supply chain technology. 2021, Gartner 2021, https://www.gartner.com/.

[36] Hassija V, Chamola V, Gupta V, Jain S, Guizani N. A survey on supply chain security: Application areas, security threats, and solution architectures. IEEE Internet Things J 2021;8(8):6222–46. http://dx.doi.org/10.1109/JIOT.2020.3025775.

[37] Lajimi C, Boufaied A, Korbaa O. Monitoring dynamic risk evolutions in operational flows of a supply chain. In: 2015 4th International Conference on Advanced Logistics and Transport (ICALT). 2015, p. 88–93. http://dx.doi.org/10.1109/ICAdLT.2015.7136599.

[38] Lehtonen M, Staake T, Michahelles F. From identification to authentication–a review of RFID product authentication techniques. Netw RFID Syst Lightweight Cryptogr 2008;169–87.

[39] Kerschbaum F, Sorniotti A. RFID-based supply chain partner authentication and key agreement. In: Proceedings of the second ACM conference on wireless network security; 2009. p. 41–50.

[40] Boyens J, Paulsen C, Moorthy R, Bartol N. Supply chain risk management practices for federal information systems and organizations. 2015, NIST SP 800-61, https://nvlpubs.nist.gov/.

[41] Rubio JE, Alcaraz C, Roman R, Lopez J. Current cyber-defense trends in industrial control systems. Comput Secur 2019;87:101561. http://dx.doi.org/10.1016/j.cose.2019.06.015, https://www.sciencedirect.com/science/article/pii/S0167404819301245.

[42] Rubio JE, Alcaraz C, Roman R, Lopez J. Analysis of intrusion detection systems in industrial ecosystems. In: 14th international conference on security and cryptography (SECRYPT 2017). 6, SciTePress; 2017, p. 116–28. http://dx.doi.org/10.5220/0006426301160128.

[43] ISO. Specification for security management systems for the suypply chain. 2007, ISO 28000, https://www.en-standard.eu/.

[44] Alcaraz C, Bernieri G, Pascucci F, Lopez J, Setola R. Covert channels-based stealth attacks in industry 4.0. IEEE Syst J. 2019;13:3980–8. http://dx.doi.org/10.1109/JSYST.2019.2912308, https://ieeexplore.ieee.org/document/8715420?source=authoralert.

[45] Bozarth CC, Warsing DP, Flynn BB, Flynn EJ. The impact of supply chain complexity on manufacturing plant performance. J Oper Manage 2009;27(1):78–93. http://dx.doi.org/10.1016/j.jom.2008.07.003, https://www.sciencedirect.com/science/article/pii/S0272696308000570.

[46] Shahid A, Almogren A, Javaid N, Al-Zahrani FA, Zuair M, Alam M. Blockchain-based agri-food supply chain: A complete solution. IEEE Access 2020;8:69230–43.

[47] Chang SE, Chen Y-C, Lu M-F. Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process. Technol Forecast Soc Change 2019;144:1–11.

[48] Conway E, Luu N, Shaffer E. Best practices in cyber supply chain risk management. NIST; 2021, https://nvlpubs.nist.gov/.

[49] Skouloudi C, Malatras A, Naydenov R, Dede G. Guidelines for securing the Internet of Thing - secure supply chain for IoT. ENISA; 2020, https://www.enisa.europa.eu.

[50] ECSO-Working Group 1. Standarization, certification and supply chain management. ECSO; 2021, https://ecs-org.eu.

[51] Gould JE, Macharis C, Haasis H-D. Emergence of security in supply chain management literature. J Transp Secur 2010;3(4):287–302.

[52] Sforzin A. Requirements Analysis of Demonstration Cases. CyberSec4Europe; 2020, https://cybersec4europe.eu/wp-content/uploads/2020/06/D5.1-Requirements-Analysis-of-Demonstration-Cases-Phase-1-v3.0.pdf, [Online; accessed 04-November-2020].

[53] Camenisch J, Van Herreweghen E. Design and implementation of the idemix anonymous credential system. In: Proceedings of the 9th ACM conference on computer and communications security; 2002. p. 21–30.

[54] Camenisch J, Fischer-Hübner S, Rannenberg K. Privacy and Identity Management for Life. Springer Science & Business Media; 2011.

[55] Sabouri A, Krontiris I, Rannenberg K. Attribute-based credentials for trust (ABC4trust). In: International conference on trust, privacy and security in digital business. Springer; 2012, p. 218–9.

[56] Ruoti S, Andersen J, Monson T, Zappala D, Seamons K. A comparative usability study of key management in secure email. In: Fourteenth symposium on usable privacy and security (SOUPS 2018). Baltimore, MD: USENIX Association; 2018, p. 375–94, https://www.usenix.org/conference/soups2018/presentation/ruoti.

[57] Alpár G, Hoepman J-H, Siljee J. The identity crisis. security, privacy and usability issues in identity management. 2011, ArXiv Preprint ArXiv:1101.0427.

[58] Moreno RT, Rodríguez JG, López CT, Bernabe JB, Skarmeta A. OLYMPUS: A distributed privacy-preserving identity management system. In: 2020 global Internet of Things summit (GIoTS). IEEE; 2020, p. 1–6.

[59] Cloudfare; 2020, https://www.cloudflare.com/, [Online; accessed 09-July-2020].

[60] Privacy Pass; 2020, https://privacypass.github.io/, [Online; accessed 09-July-2020].

[61] Credential; 2020. https://credential.eu//, [Online; accessed 09-July-2020].

[62] Lorünser T, Rodriguez CB, Demirel D, Fischer-Hübner S, Groß T, Länger T, et al. Towards a new paradigm for privacy and security in cloud services. In: Cyber security and privacy forum. Springer; 2015, p. 14–25.

[63] Wästlund E, Angulo J, Fischer-Hübner S. Evoking comprehensive mental models of anonymous credentials. In: International workshop on open problems in network security. Springer; 2011, p. 1–14.

[64] Alaqra AS, Fischer-Hübner S, Framner E. Enhancing privacy controls for patients via a selective authentic electronic health record exchange service: qualitative study of perspectives by medical professionals and patients. J Med Internet Res 2018;20(12):e10954.

[65] European Central Bank. Record of processing activity – reporting framework for cyber incidents on significant institutions. 2020, https://www.ecb.europa.eu/ecb/access_to_documents/data_protection/shared/pdf/ecb.dpr.dgms4_reporting_cyber_incidents_significant_institutions20200224.en.pdf, [Online; accessed 04-November-2020].

[66] Georgia Bafoutsou MD. Telecom services security incidents 2019 annual analysis report. Technical report, ENISA; 2020, https://www.enisa.europa.eu/publications/annual-report-telecom-security-incidents-2019/at_download/fullReport, [Online; accessed 08-November-2020].

[67] NCSC. National cyber security centre – reporting a cyber security incident. 2020, https://report.ncsc.gov.uk/, [Online; accessed 21-October-2020].

[68] CISA. Cybersecurity & infrastructure agency – report incidents, phishing, malware, or vulnerabilities. 2020, https://us-cert.cisa.gov/forms/report, [Online; accessed 21-October-2020].

[69] DHS. Cyber incident reporting: A unified message for reporting to the federal government. 2020, https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf, [Online; accessed 21-October-2020].

[70] Converge. Cyber incident reporting guidelines: What you need to know. 2020, https://www.convergetechmedia.com/cyber-incident-reporting-guidelines-need-know/, [Online; accessed 21-October-2020].

[71] L. Pupillo GV. Software vulnerability disclosure in Europe: Technology, policies and legal challenges. Technical Report, CEPS; 2018, https://www.ceps.eu/ceps-publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges/, [Online; accessed 08-November-2020].

[72] Naseer H, Maynard SB, Desouza KC. Demystifying analytical information processing capability: The case of cybersecurity incident response. Decis Support Syst 2021;143:113476. http://dx.doi.org/10.1016/j.dss.2020.113476, https://www.sciencedirect.com/science/article/pii/S0167923620302311.

[73] Van der Kleij R, Kleinhuis G, Young H. Computer security incident response team effectiveness: A needs assessment. Front Psychol 2017;8:2179. http://dx.doi.org/10.3389/fpsyg.2017.02179, https://www.frontiersin.org/article/10.3389/fpsyg.2017.02179.

[74] Catota FE, Morgan MG, Sicker DC. Cybersecurity incident response capabilities in the ecuadorian financial sector. J Cybersecur 2018;4(1). http://dx.doi.org/10.1093/cybsec/tyy002, tyy002.

[75] Ahmad A, Maynard SB, Desouza KC, Kotsias J, Whitty MT, Baskerville RL. How can organizations develop situation awareness for incident response: a case study of management practice. Comput Secur 2021;101:102122. http://dx.doi.org/10.1016/j.cose.2020.102122, https://www.sciencedirect.com/science/article/pii/S0167404820303953.

[76] Ab Rahman NH, Choo K-KR. A survey of information security incident handling in the cloud. Comput Secur 2015;49:45–69. http://dx.doi.org/10.1016/j.cose.2014.11.006, https://www.sciencedirect.com/science/article/pii/S0167404814001680.

[77] Sarker I, Kayes A, Badsha S, et al. Cybersecurity data science: an overview from machine learning perspective. J Big Data 2020;7(41). http://dx.doi.org/10.1186/s40537-020-00318-5.

[78] Schauer S, Kalogeraki E-M, Papastergiou S, Douligeris C. Detecting sophisticated attacks in maritime environments using hybrid situational awareness. In: 2019 international conference on information and communication technologies for disaster management (ICT-DM). IEEE; 2019, p. 1–7.

[79] Lehto M. Cyber security in aviation, maritime and automotive. In: Computation and big data for transport. Springer; 2020, p. 19–32.

[80] Tam K, Jones KD. Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. J Cyber Policy 2018;3(2):147–64.

[81] Gcaza N, Von Solms R. A strategy for a cybersecurity culture: A South African perspective. Electron J Inf Syst Dev Countries 2017;80(1):1–17.

[82] Da Veiga A. A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. In: 2016 SAI computing conference (SAI). IEEE; 2016, p. 1006–15.

[83] EU Commission. Blueprint for coordinated response to large-scale cross-border cybersecurity incidents and crises. 2017, https://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-6100-F1-EN-ANNEX-1-PART-1.PDF, [Online; accessed 08-November-2020].

[84] ENISA. Cyber security and resilience for smart hospitals. 2016, https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals, [Online; accessed 08-November-2020].

[85] ENISA. Procurement guidelines for cybersecurity in hospitals. 2020, https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals, [Online; accessed 08-November-2020].

[86] Coventry L, Branley D. Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas 2018;113:48–52.

[87] Nalin M, Baroni I, Faiella G, Romano M, Matrisciano F, Gelenbe E, et al. The European cross-border health data exchange roadmap: Case study in the Italian setting. J Biomed Inform 2019;94:103183.

[88] Abdellatif AA, Samara L, Mohamed A, Erbad A, Chiasserini CF, Guizani M, et al. Medge-chain: Leveraging edge computing and blockchain for efficient medical data exchange. IEEE Internet Things J 2021.

[89] Xia Q, Sifah EB, Asamoah KO, Gao J, Du X, Guizani M. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access 2017;5:14757–67.

[90] European Data Protection Board. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. 2020, https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf, [Online; accessed 03-May-2021].

[91] European Data Protection Supervisor. Preliminary opinion 8/2020 on the European health data space. 2020, https://edps.europa.eu/sites/default/files/publication/20-11-17_preliminary_opinion_european_health_data_space_en.pdf, [Online; accessed 03-May-2021].

[92] Larrucea X, Moffie M, Asaf S, Santamaria I. Towards a GDPR compliant way to secure European cross border healthcare industry 4.0. Comput Stand Interfaces 2020;69:103408.

[93] Mohammadi F, Panou A, Ntantogian C, Karapistoli E, Panaousis E, Xenakis C. CUREX: Secure and private health data exchange. In: IEEE/WIC/ACM international conference on web intelligence-companion volume; 2019, p. 263–68.
[94] Jin H, Luo Y, Li P, Mathew J. A review of secure and privacy-preserving medical data sharing. IEEE Access 2019;7:61656–69.
[95] Martucci LA, Fischer-Hübner S, Hartswood M, Jirotka M. Privacy and social values in smart cities. In: Designing, developing, and facilitating smart cities. Springer; 2017, p. 89–107.
[96] Cui L, Xie G, Qu Y, Gao L, Yang Y. Security and privacy in smart cities: Challenges and opportunities. IEEE Access 2018;6:46134–45. http://dx.doi.org/10.1109/ACCESS.2018.2853985.
[97] Gharaibeh A, Salahuddin MA, Hussini SJ, Khreishah A, Khalil I, Guizani M, Al-Fuqaha A. Smart cities: a survey on data management, security, and enabling technologies. IEEE Communications Surveys Tutorials 2017;19(4):2456–501. http://dx.doi.org/10.1109/COMST.2017.2736886.
[98] Tabassi E, Burns K, Hadjimichael M, Molina-Markham A, Sexton J. A taxonomy and terminology of adversarial machine learning. 2019, NIST IR.
[99] Apruzzese G, Colajanni M, Ferretti L, Marchetti M. Addressing adversarial attacks against security systems based on machine learning. In: 2019 11th international conference on cyber conflict (CyCon). 900, IEEE; 2019, p. 1–18.
[100] Biggio B, Roli F. Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognit 2018;84:317–31.
[101] Shahraeini M, Kotzanikolaou P. A dependency analysis model for resilient wide area measurement systems in smart grid. IEEE J Sel Areas Commun 2019;38(1):156–68.
[102] Berkeley AR, Wallace M, COO C. A framework for establishing critical infrastructure resilience goals. Final Report and Recommendations By the Council, National Infrastructure Advisory Council; 2010.
[103] Cabinet Office. Keeping the country running: natural hazards and infrastructure. 2011, Improving the UK's Ability To Absorb, Respond To and Recover from Emergencies.
[104] Kumar RSS, Nyström M, Lambert J, Marshall A, Goertzel M, Comissoneru A, et al. Adversarial machine learning-industry perspectives. In: 2020 IEEE security and privacy workshops (SPW). IEEE; 2020, p. 69–75.
[105] Markatos E. Research and development roadmap 1. CyberSec4Europe; 2020, https://cybersec4europe.eu/wp-content/uploads/2020/09/D4.3-Roadmap-v5-NEW.pdf, [Online; accessed 04-November-2020].
[106] Dragoni N. Education and Training Review. CyberSec4Europe; 2020, https://cybersec4europe.eu/wp-content/uploads/2020/02/D6.2-Education-and-Training-Review-V1.2-Submtted.pdf, [Online; accessed 04-November-2020].
[107] Skarmeta A. Common framework handbook 1. CyberSec4Europe; 2020, https://cybersec4europe.eu/wp-content/uploads/2020/06/D3.1-Handbook-v2.0-submitted-1.pdf, [Online; accessed 04-November-2020].

**Simone Fischer-Hübner** received the Diploma degree in computer science (law), in 1988, and the Ph.D. and Habilitation degrees in computer science from the University of Hamburg, Germany, in 1992 and 1999, respectively. She has been a Full Professor with Karlstad University, Sweden, since 2000, where she is currently the Head of the Privacy and Security Research Group. Her research interests include cybersecurity, privacy-enhancing technologies, and useable privacy and security. She is a Swedish IFIP TC 11 Representative, IFIP TC-11 Vice Chair and a member of the Advisory Board Swedish Civil Contingency Agency's Cyber Security Council. She serves as the Vice Chair for the IEEE Sweden Computer/Software Engineering Chapter.

**Cristina Alcaraz** is an Associate Professor in the Department of Computer Science, University of Malaga. Her main research interests include critical infrastructure protection, and more specifically with the security of SCADA systems, cyber–physical systems, industrial Internet of Things and digital twins; all of them applied in Industry 4.0, manufacturing and supply chain systems and smart grids.

**Afonso Ferreira** has held European leadership roles in institutional policy and research, including at the European Commission. He holds a PhD in Computer Science and is Directeur de Recherche with the French CNRS, being the head of European and International ICT research. Afonso leads his lab's participation in a pilot for the upcoming European legislation in Cybersecurity. He worked in the areas of Communication Networks, HPC, and Algorithms, having published more than 100 papers in the forefront of scientific research. He participated in more than 70 Technical Committees and sits in editorial boards of international journals. More information at www.linkedin.com/in/cyberfuture.

**Carmen Fernandez-Gago** is an associate professor at the University of Malaga. She obtained a degree in Mathematics from the University of Málaga (Spain) and holds a Ph.D. in Computer Science from the University of Liverpool (United Kingdom), where she also worked as a postdoctoral researcher. In January 2006, she joined the NICS lab at the department of Computer Science of the University of Malaga where she has carried out her research. Her main research interests are in the area of trust and reputation management systems. She has published many research papers in this area and has organised and is a member of several program committees for international conferences in the area. She has also worked in several national and European projects.

**Javier Lopez** is a Full Professor at the University of Malaga and Head of the Network, Information and Computer Security Laboratory (NICS Lab). His research activities focus on network & information security and Critical Information Infrastructures. He is currently Editor-in-Chief of the International Journal of Information Security, and member of the editorial boards of the journals Computers & Security, IET Information Security, IEEE Wireless Communication, Journal of Computer Security, and IEEE Internet of Things Journal, amongst others. Prof. Lopez is the Spanish representative at IFIP Technical Committee 11 Security and Protection in Information Processing Systems.

**Evangelos Markatos** is a professor of Computer Science at the University of Crete. He received his diploma in Computer Engineering from the University of Patras and the M.Sc. and Ph.D. in Computer Science from the University of Rochester. He has co-authored more than 150 publications in top conferences and journals including ACM SOSP, IEEE HPCA, ACM/IEEE ToN, IEEE JSAC, USENIX Security, INFOCOM, etc. According to Google Scholar his work has received close to 8,000 citations with an h-index of 45.

**Lejla Islami** received the M.Sc. degree in cybersecurity, specialising in digital forensics from Tallinn University of Technology and University of Tartu, Estonia. She is currently pursuing the Ph.D. degree in computer science with Karlstad University, Sweden. Her current work focuses on investigating users' privacy perceptions and requirements on vehicular communication systems. Her research interests expand over disciplines of HCI, useable privacy, IoT, cybersecurity and nationwide cyber awareness.

**Mahdi Akil** received his bachelor degree in computer science from the Lebanese International University, Lebanon in 2015. And his master's degree in networks and security from Sapienza University of Rome, Italy in 2018. He is currently pursuing the Ph.D. degree with the department of computer science at Karlstad university, Sweden. His research interests include security and privacy in vehicular ad hoc networks and smart environments.