Horizon 2020 Program (2014-2020)

Cybersecurity, Trustworthy ICT Research & Innovation Actions
Security-by-design for end-to-end security
H2020-SU-ICT-03-2018

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

Cyber security cOmpeteNCe fOr Research anD InnovAtion [†]

Work Package 4: Policy and the European Dimension Preliminary Version of Deliverable D 4.4: Cybersecurity Roadmap for Europe by CONCORDIA

Abstract: This document describes the preliminary version of the deliverable D4.4 and with this the current status of CONCORDIA's work on the Cybersecurity Roadmap for Europe.

[†] This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830927.

Contractual date of delivery	*Date as listed in the DoA as 31.12.2022*
Actual date of delivery	*31.12.2020*
Deliverable dissemination level	*Public*
Editors	*Gabi Dreo (UniBW/CODE)* *Corinna Schmitt (UniBW/CODE)* *Arthur van der Wees (Arthur's Legal)*
Contributors	*Neeraj Suri (ULANC)* *Luis Barriga (Ericsson)* *Muriel Franco (UZH)* *Burkhard Stiller (UZH)* *Felicia Cutas (EIT DIGITAL)* *Kostas Lampropoulos (UP)* *Claudio Ardagna (UMIL)* *Arthur Van der Wees (ARTHUR'S LEGAL)* *Dimitra Stefanatou (ARTHUR'S LEGAL)* *Argyro Chatzopoulous (TÜV TRUST IT)* *Gabi Dreo (UniBW/CODE)* *Aiko Pras (UT)* *Michael Sirivianos (CUT)* *Jean-Yves Marion (UL)* *Cristian Hesselman (SIDN)*
Quality assurance	*Tatjana Welzer Družovec (University of Maribor)* *Urška Kežmah (University of Maribor)* *Paolo de Lutiis (Telecom Italia)* *Ovidiu Costel Mihaila (Bitdefender)* *Ernesto Damiani (University of Milan)*

The CONCORDIA Consortium

UniBW/CODE	University Bundeswehr Munich / Research Institute CODE (Coordinator)	Germany
FORTH	Foundation for Research and Technology - Hellas	Greece
UT	University of Twente	Netherlands
SnT	University of Luxembourg	Luxembourg
UL	University of Lorraine	France
UM	University of Maribor	Slovenia
UZH	University of Zurich	Switzerland
JACOBSUNI	Jacobs University Bremen	Germany
UI	University of Insubria	Italy
CUT	Cyprus University of Technology	Cyprus
UP	University of Patras	Greece
TUBS	Technical University of Braunschweig	Germany
~~TUDA~~	~~Technical University of Darmstadt~~	~~Germany~~
MU	Masaryk University	Czech Republic
BGU	Ben-Gurion University	Israel
OsloMET	Oslo Metropolitan University	Norway
Imperial	Imperial College London	UK
UMIL	University of Milan	Italy
BADW-LRZ	Leibniz Supercomputing Centre	Germany
EIT DIGITAL	EIT DIGITAL	Belgium
TELENOR ASA	Telenor ASA	Norway
AirbusCS-GE	Airbus Cybersecurity GmbH	Germany
SECUNET	secunet Security Networks AG	Germany
IFAG	Infineon Technologies AG	Germany
SIDN	Stichting Internet Domeinregistratie Nederland	Netherlands
SURFnet bv	SURFnet bv	Netherlands
CYBER-DETECT	Cyber-Detect	France
TID	Telefonica I+D SA	Spain
RUAG	RUAG AG (as replacement for RUAG Schweiz AG)	Switzerland
BITDEFENDER	Bitdefender SRL	Romania
ATOS	Atos Spain S.A.	Spain
SAG	Siemens AG	Germany
Flowmon	Flowmon Networks AS	Czech Republic
TÜV TRUST IT	TUV TRUST IT GmbH	Germany
TI	Telecom Italia SPA	Italy
Efacec	EFACEC Electric Mobility SA (as replacement for EFACEC Energia)	Portugal
ARTHUR'S LEGAL	Arthur's Legal B.V.	Netherlands
eesy-inno	eesy-innovation GmbH	Germany
DFN-CERT	DFN-CERT Services GmbH	Germany
CAIXABANK SA	CaixaBank SA	Spain
~~BMW Group~~	~~Bayerische Motoren Werke AG~~	~~Germany~~
GSDP	Ministry of Digital Policy, Telecommunications and Media	Greece
RISE	RISE Research Institutes of Sweden AB	Sweden
Ericsson	Ericsson AB	Sweden
SBA	SBA Research gemeinnutzige GmbH	Austria
IJS	Institut Jozef Stefan	Slovenia

UiO	University of Oslo	Norway
ULANC	University of Lancaster	UK
ISI	ATHINA-ISI	Greece
UNI PASSAU	University of Passau	Germany
RUB	Ruhr University Bochum	Germany
CRF	Centro Ricerche Fiat	Italy
ELTE	EOTVOS LORAND TUDOMANYEGYETEM	Hungary
Utimaco	Utimaco managment GmbH	Germany

Document Revisions & Quality Assurance

Internal Reviewers

1. Tatjana Welzer Druzovec (University of Maribor) (review lead)
2. Paolo de Lutiis (Telecom Italia)
3. Ovidiu Costel Mihaila (Bitdefender)
4. Ernesto Damiani (University of Milan)

Revisions

Ver.	Date	By	Overview
0.01	*23.09.2020*	*Neeraj Suri (ULANC)*	*Initial draft including i.e. economics, legal, and technology aspects*
0.02	*24.09.2020*	*Luis Barriga (Ericsson)*	*Updating technology part*
0.03	*27.09.2020*	*Corinna Schmitt (UniBW/CODE)*	*Restructure of the TOC and expanding content regarding challenges and objectives in different sections; added ideas from brainstorming (marked yellow)*
0.04	*29.10.2020*	*Ivana Buntic-Ogor (UniBW/CODE)*	*Formatting text, references and figures*
0.05	*03.11.2020*	*Ivana Buntic-Ogor (UniBW/CODE)*	*Updated structure*
0.06	*04.11.2020*	*Ivana Buntic-Ogor (UniBW/CODE)*	*Further updated structure*
0.07	*11.11.2020*	*Muriel Franco (UZH)*	*Added inputs for Economic Perspectives (Section 6)*
0.08	*12.11.2020*	*Felicia Cutas (EIT DIGITAL)*	*first draft text on Education*
0.09	*12.11.2020*	*Claudio Ardagna (UMIL)*	*first draft of Chapter 3*
0.10	*13.11.2020*	*Arthur Van der Wees (ARTHUR'S LEGAL)*	*Initial Input Chapter 7*
0.11	*13.11.2020*	*Arthur Van der Wees (ARTHUR'S LEGAL), Corinna Schmitt (UniBW/CODE)*	*Further Input Chapter 7, adding two more chapters*
0.12	*16.11.2020*	*Argyro Chatzopoulou (TÜV TRUST IT)*	*Initial Input Chapter 8*
0.13	*24.11.2020*	*Corinna Schmitt (UniBW/CODE)*	*Input harmonized*
0.14	*26.11.2020*	*Claudio Ardagna (UMIL)*	*First complete draft of Chapter 3*
0.15	*26.11.2020*	*Felicia Cutas (EIT DIGITAL)*	*Update Chapter 5*
0.16	*26.11.2020*	*Ivana Buntic-Ogor (UniBW/CODE)*	*Input harmonized*
0.17	*26.11.2020*	*Ivana Buntic-Ogor (UniBW/CODE)*	*Formatting, References resolved*
0.18	*27.11.2020*	*Corinna Schmitt (UniBW/CODE)*	*Initial Input Chapter 2*
0.19	*27.11.2020*	*Arthur Van der Wees (ARTHUR'S LEGAL), Corinna Schmitt (UniBW/CODE)*	*Further input to Chapters 7, 9, 10; formatting*
0.20	*27.11.2020*	*Felicia Cutas (EIT DIGITAL)*	*further input on Chapter 5*
0.21	*30.11.2020*	*Ivana Buntic-Ogor (UniBW/CODE)*	*Formatting*
0.22	*01.12.2020*	*Corinna Schmitt, Gabi Dreo (UniBW/CODE)*	*Introduction, Chapter 2*
0.23	*02.12.2020*	*Ivana Buntic-Ogor (UniBW/CODE)*	*Formatting*
0.24	*03.12.2020*	*Claudio Ardagna (UMIL)*	*Minor comments on chapter 3*
0.25	*04.12.2020*	*Gabi Dreo (UniBW/CODE)*	*Chapter 1 and 2*
0.26	*04.12.2020*	*Burkhard Stiller (UZH)*	*Updates in Chapter 6*
0.27	*07.12.2020*	*Arthur van der Wees (ARTHUR'S LEGAL)*	*Further input to Chapters 1, 2, 5, 7, 9 and 10*
0.28	*07.12.2020*	*Felicia Cutas (EIT DIGITAL)*	*Chapter 5 updated*
0.29	*07.12.2020*	*Arthur van der Wees (ARTHUR'S LEGAL)*	*Further input to Chapters 6, 7, 9 and 10*
0.30	*07.12.2020*	*Gabi Dreo (UniBW/CODE)*	*Executive, Intro updates*
0.31	*08.12.2020*	*Arthur van der Wees (ARTHUR'S LEGAL)*	*Visuals/Figures numbered, and references/links corrected*
0.32	*09.12.2020*	*Argyro Chatzopoulou (TÜV TRUST IT), Gabi Dreo (UniBW/CODE)*	*Update on timeline Chapter 8, Updates in several Chapters*
0.33	*10.12.2020*	*Aiko Pras (UT)*	*Chapter 4*

Ver.	Date	By	Overview
0.34	*11.12.2020*	*Argyro Chatzopoulou (TÜV TRUST IT), Aiko Pras (UT), Kostas Lampropoulos (UP), Felicia Cutas (EIT DIGITAL)*	*Additions to Chapter 8, Update Chapter 4, Comments and update Chapter 5*
0.35	*11.12.2020*	*Felicia Cutas (EIT DIGITAL)*	*Figures update Chapter 5*
0.36	*18.12.2020*	*Arthur van der Wees (ARTHUR'S LEGAL)*	*Changes, update figures*
0.36a	*18.12.2020*	*Corinna Schmitt (UniBW/CODE)*	*Transfer to Latex, footnotes to references*
0.37	*18.12.2020*	*Aiko Pras (UT)*	*Chapter 4 (updates, figure)*
0.38	*18.12.2020*	*Ivana Buntic-Ogor (UniBW/CODE)*	*Figures fix*
0.39	*18.12.2020*	*Marinos Tsantekidis (TUBS)*	*Chapter 4*
0.40	*21.12.2020*	*Corinna Schmitt (UniBW/CODE)*	*Creation Acronym list*
0.41	*22.12.2020*	*Arthur van der Wees (ARTHUR'S LEGAL)*	*review addressed and additions*
0.42	*24.12.2020*	*Corinna Schmitt (UniBW/CODE)*	*review addressed*

Disclaimer:
The sole responsibility of this document lies with the authors. The European Commission is not responsible for any use that may be made of the information contained therein.

Executive Summary

All future global market-dominant products and services will be located in the digital world, in cyberspace, or at least interact strongly with it. Cybersecurity is the pillar of the digital society and the guarantee of trust and cooperation. Therefore, cybersecurity and its roadmap cannot be analysed only from a technological perspective. When discussing the cybersecurity roadmap, it is necessary to take a holistic approach having in mind the global aim of European digital sovereignty.

In an increasingly globalised world, Europe presents itself as a champion of European ethical values but cannot guarantee the digital sovereignty of its citizens or its businesses. Even current challenges in the field of climate protection and health, especially concerning the COVID-19 pandemic, can only be solved or supported by using trustworthy IT to prevent that Europe ends as a digital colony. Building the European digital ecosystems with various stakeholders, identifying synergies, strengthening trust and cooperation, investing in digital competencies and the European IT industry are pillars to build a strong digital sovereign Europe. CONCORDIA's roadmap addresses these various aspects.

Work Package 4 (WP4) is organised into several tasks. The present document D4.4 is a first draft deliverable of Task 4.4 that presents a draft version of the "Cybersecurity Roadmap for Europe by CONCORDIA" based on the state of play up to and including 12 December 2020. As agreed with the reviewers and the project officer, it will be submitted to the reviewing process in a draft version to provide insights into the current work concerning the definition of the roadmap. The final version of the deliverable is planned for M48. The specification of the roadmap is not driven only from the internal discussion, discussions with the CONCORDIA's Advisory Board, or conferences such as the CONCORDIA Open Door 2020 or the CODE 2020. Besides, it is planned to incorporate the insights from other pilots in the next versions of the deliverable as more advanced input is available from the other pilots.

Among the key achievements of deliverable D4.4 is the holistic approach to the definition of the Cybersecurity Roadmap for Europe by CONCORDIA, and the identification of the six dimensions of observation, namely (i) Research and Innovation, (ii) Education and Skills, (iii) Legal and Policy, (iv) Economics and Investments, (v) Certification and Standardization and (vi) Community Building. It is not enough to focus only on the technological aspects (i.e., technological sovereignty) but has in mind also other dimensions and the interdependencies between them. For example, research and innovation can only be achieved with strong digital competencies (i.e., education and skills dimension) and investments (i.e., economics and investments dimension). These recommendations of the roadmaps are put on the time scale from short-term (next two, three years), mid-term (around 2025), and long-term (around 2030). The general aim of this roadmap is to both identify and jointly work to addressing, mitigating (and even resolving) the challenges regarding European digital sovereignty, overcoming fragmentation while identifying and

joining European brainpower and forces to build, boost and amplify the gains of (the road towards) building, achieving and sustaining European digital sovereignty.

As this is a dynamic, ever-changing and expanding dimension that affects almost everything, this current release of the Roadmap can be deemed to be a rolling release, with its current state of play as per 12th of December, 2020.

The progress of the specification of the roadmap is progressing according to plan. All milestones have been reached. There are no deviations encountered so far, also with respect to the COVID-19 pandemic.

Contents

1 Introduction

Work Package 4 (WP 4) entitled ‘Standardization, Liaison, Economic aspects, Cybersecurity research map’ has several tasks and deliverables for M24. This draft deliverable D4.4 addresses the outcome of T4.4, which is devoted to the specification of a ‘Cybersecurity Roadmap for Europe by CONCORDIA’.

As already described in the DoA, CONCORDIA is committed to following a holistic approach in the development of the **Cybersecurity Roadmap for Europe by CONCORDIA** with the focus on building, achieving, and sustaining European Digital Sovereignty. A holistic approach requires analysing the goal from various dimensions. CONCORDIA identifies six dimensions as (i) Research and Innovation, (ii) Education and Skills, (iii) Legal and Policy, (iv) Economics and Investments, (v) Certification and Standardization, and (vi) Community Building. To precisely address the specifics of each dimension, a separate roadmap is developed within each dimension. Since the dimensions are interconnected, so are the roadmaps, too.

Furthermore, where digital technology, systems, and services are growing at an unprecedented rate, the global COVID-19 pandemic has further accelerated their adoption in the European Union and all across the globe – sometimes up to more than 1.000% increase –, further unbalancing digital sovereignty (as also confirmed in the ENISA Threat Landscape 2020, published in October 2020), including without limitations adding to a rise of digital feudalism and decrease of wealth distribution. In addition, digital sovereignty is analysed from other perspectives such as sustainability and green technologies. Also in this context, the need to bolster digital sovereignty is further underscored.

The general aim of this Roadmap is to both identify and jointly work to addressing, mitigating (and even resolving) the challenges regarding European digital sovereignty while identifying and joining European brainpower and forces to build, boost and amplify the gains of (the road towards) building, achieving and sustaining European digital sovereignty. As this is a dynamic, ever-changing and expanding dimension that affects almost everything, this current release of the Roadmap can be deemed to be a rolling release, with its current state of play as per December 2020.

1.1 Structure of the Document

The structure of the deliverable is as follows. It starts with motivating the CONCORDIA’s holistic approach in defining the roadmap, being the six dimensions of observation, namely (i) Research and Innovation, (ii) Education and Skills, (iii) Legal and Policy, (iv) Economics and Investments, (v) Certification and Standardization and (vi) Community Building, are discussed in Chapter 2. An essential step towards the specification of the roadmaps is an analysis of the threat landscape from device-centric to user-centric security, as done in Chapter 3 , including an analysis of the influence of COVID-19 in the last 9 months. The chapter is concluded by listing technology stack-related recommendations. Chapter 4 focuses on the first dimension, which is to develop a **Roadmap for Research and Innovation**, starting with identifying challenges and technological areas that need to be addressed, aligned on the timeline of short, mid, and long term. Chapter 5 focuses on the next dimension, which is the **Roadmap for Education and Skills**. Another dimension to address is the economic field and investments addressed in Chapters 6 and 7 with the **Roadmap for Economics and Investments**. Another perspective is represented by the legal and policy dimension addressed in Chapter 8 with the **Roadmap for Legal and Policy**. For the acceptance of the technology on the market and acceptance on the political floor establishing new regulations, it is essential to foster certification and standardization. This requirement is addressed in Chapter 9 with the **Roadmap for Certification and Standardization**. Chapter 10 addresses the objective to specify a **Roadmap for Community Building** and building the European digital ecosystems. Finally, strengthening digital sovereignty means also enabling Europe's tween transitions to a green and digital economy. Chapter 11 addresses therefore also other aspects such as sustainability and green technologies.

2 A Holistic Approach towards European Digital Sovereignty resp. Strategic Autonomy

All future global market-dominant products, systems, and services will be located in the digital world, in cyberspace, cyber-physical, or at least interact strongly with it to some extent. Examples are robotics, industrial automation, autonomous driving, intelligent power networks, smart urban society, smart grids, and smart homes. Digital technologies such as Big Data, Artificial Intelligence, and cyber-physical systems generate and process huge amounts of data generated in these areas. The data and digital services are currently dominated almost exclusively by non-European players, in particular American and, increasingly, Chinese global players.

The COVID-19 pandemic crisis has affected our daily lives. Another phenomenon, however, has already - and will in all probability continue to - cause even more serious changes: digitalization. Like the spread of viruses, digital technology is developing exponentially. It is changing the economic strength of entire nations. It will change the face of our economy, but also our culture, our civil society, the politics, and the life of every individual more lastingly than any other technology before. At present, especially in Europe, digital technology is perceived as an environmental phenomenon similar to the weather. It's coming, there's little or nothing you can do about it. Thus, we accept it and use it as far as it is attractive - and many things are attractive - but we do not design it. This already has more consequences today but will have fatal consequences in the future. Europe is already largely a digital developing union and on the way to becoming a digital colony. This is seen as inevitable by (too) many managers. Europe's conventional companies are already economically endangered in the medium term anyway - by the large digital platform companies. To believe that they can be protected by keeping them out of customs restrictions is a fatal error. Especially without any regulation, the large digital companies will become an economically brute force.

In an increasingly globalized world, Europe presents itself as a champion of European ethical values, but this cannot guarantee the digital sovereignty of its citizens, its communities, companies, organisations and member states, allies, and friends. Even current challenges in the area of climate protection and health, currently especially with regard to the COVID-19 pandemic, can only be solved or supported with trustworthy IT. There is no alternative to digitalization.

The question 'Who is prepared for the new Digital Age' has been put rightfully on the agenda, including the reconfirmation that the adoption of digital technologies in Europe is relatively slow, including that European firms are lagging behind, this also as reported by the European Investment Bank [1]. There is a lot at stake, including our European digital sovereignty.

Digital sovereignty is a multi-layered and complex concept. There are a number of related terms such as 'technological sovereignty', 'strategic autonomy', 'self-sovereignty', 'data-sovereignty', and 'digital autonomy'. As summarized in the EPRS Ideas Paper [2] from the European Parliament to overcome this situation it '*would require the Union to update and adapt a number of its current legal, regulatory and financial instruments, and to promote more actively European values and principles in areas such as data protection, cybersecurity and ethically designed artificial intelligence (AI).*' With this, the European Parliament identified the emerging request for **digital sovereignty** referring to '**Europe's ability to act independently in the digital world** [3] and should be understood in terms of both protective mechanisms and offensive tools to foster digital innovation (including in cooperation with non-EU companies).' [2]

Digital sovereignty can also be defined out of the negatives: not to be further developed as or become a digital colony; not to facilitate the rise of digital feudalism, and not further to losing control over European human values, and not further losing control, ownership, and benefits of the value, accessibility, use and accuracy of our data, attributes, information knowledge, and experience.

ENISA [4] has addressed the aspect of European digital sovereignty especially with respect to the aspect of a supply chain of cybersecurity products in Europe, as well as the relationship between the global ICT market and the cybersecurity market, and pointed out that EU is sandwiched between US and China/South Korea, as visualized in Figure 1.

Figure 1: EU sandwiched between US and China

Addressing European digital sovereignty only from a technological viewpoint and addressing just **technological sovereignty** is too narrow. For once, as technological sovereignty cannot be achieved or sustained by state of the art or cutting-edge technology itself, it will be dependent and interdependent on other aspects. For an appropriate understanding of European digital sovereignty, a holistic approach needs to be taken that embraces various different aspects. CONCORDIA follows this and takes a holistic view in developing the roadmaps to reach the aim of European digital sovereignty. Thus, in this Roadmap, we have several 'sub-'roadmaps or 'mini'-roadmaps that address specific dimensions and other aspects, and which are dependent on each other.

CONCORDIA has identified six dimensions to address a holistic view of European digital sovereignty, as depicted in Figure 2.:

1. Research and Innovation (Chapter 4)
2. Education and Skills (Chapter 5)
3. Economics and Investments (Chapters 6 and 7)
4. Legal and Policy (Chapter 8)
5. Certification and Standardization (Chapter 9)
6. Community Building (Chapter 10)

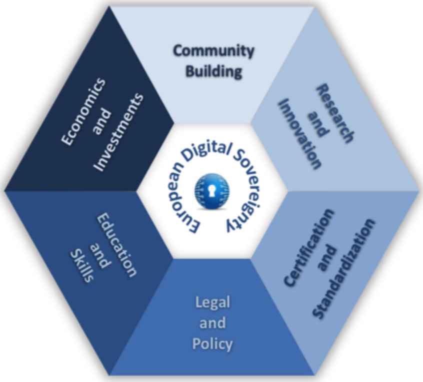

Community Building
Research and Innovation
Certification and Standardization
Legal and Policy
Education and Skills
Economics and Investments
European Digital Sovereignty

Figure 2: CONCORDIA's dimensions

Research and Innovation address the aspect of technological sovereignty. **Education and Skills** refer to the necessity to build IT and cybersecurity competences. **Legal and Policy** focus on regulation and legal aspects and strategies. Developing new digital value models, business models, and attracting investments are discussed in **Economics and Investments**. **Certification and Standardization** are playing an important role in the European cybersecurity certification framework for ICT products, services, and processes, and are addressed in this dimension. The **Community Building** dimension addresses the need to overcome the fragmentation in Europe and interconnect various stakeholders. Building digital ecosystems, interconnect different stakeholders, and with this establishing trust and cooperation is the European way to build European digital sovereignty, and not be sandwiched between US and China. The identified six dimensions are not independent of each other. Each is intertwined with the other. For example, **Research and Innovation** addressing technological sovereignty can only be successful if competences (the **Education and Skills** dimension) are addressed as well.

The discussion of the six dimensions starts with an analysis of the threat landscape.

3 Threat Landscape

Driven by digitalization, information sharing has been experiencing exponential growth in the past few years. In turn, one's eagerness to better prepare and protect depends on the ability to change the attitude from 'need to know' to 'need to share'. Digital technologies, most notably Artificial Intelligence (AI), are shaping decision-making, everyday communication, life, and work, hence highlighting the importance of maintaining the online economy and ensuring its prosperity. The continuous observation of the threat landscape is a precondition for the specification of the roadmap for cybersecurity.

The threat landscape is continuously changing and evolving to address the evolution of the IT environment from software to the Internet of Things (IoT), via services and cloud computing. Providing an up-to-date overview of cybersecurity threats and attacks is critical to provide a sound cybersecurity roadmap that evaluates new trends in cybersecurity. CONCORDIA's cybersecurity threat analysis is inspired by different research domains as follows: device-centric, network-centric, system-centric, data-/application-centric, and user-centric security.

Network-centric security refers to data transport as well as to the networking and the security issues associated with it. Topics range from DDoS (Distributed Denial of Service) protection, Software-Defined Networking (SDN), ad hoc networks to encrypted traffic analysis, cellular mobile networks. System-centric security centers around cloud and virtualized environments, while IoT/Device-centric security centers around modern systems such as IoT/edge and corresponding devices, both targeting topics such as middleware, secure OS, and security by design, malware analysis, systems security validation, detection of zero-days, and recognizing service dependencies are specifically addressed. Data-centric security addresses issues concerned with management, analysis, protection, and visualization of data at all layers of a given system/environment, focusing on modern Big Data environments. Application-centric security addresses issues related to the security of applications, like modern services and their management. User-centric security addresses issues like privacy, social networks, fake news, and identity management. The above domains apply to any environments ranging from traditional distributed IT systems to devices that produce raw data, such as embedded systems, sensors, IoT devices, drones, and the associated security-centric issues, such as IoT security, via service-based systems, such as, service-oriented architecture, cloud, microservices.

3.1 Cybersecurity Threat Overview

In this section we briefly summarize the Cybersecurity state of the art in the domains inspired by CONCORDIA's security layers illustrated in Figure 3.

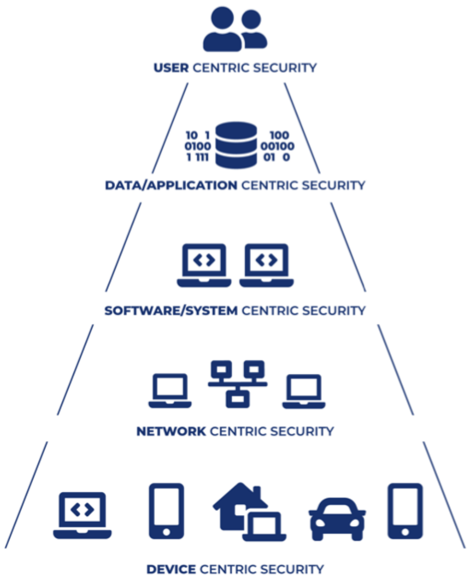


Figure 3: CONCORDIA's security layers

3.1.1 Device/IoT-Centric Security

A guide to IoT Infographic [5] presents a brief overview of the current state and future of the IoT. According to it, by the end of 2025, it is projected that there will be 200 billion objects that use wireless technology. Most of the smart devices are or will be used in factories and businesses (40.2%) and healthcare (30.3%). In those areas smart devices assist in tracking inventory, managing machines, reducing costs, and saving lives. The value of these devices is expected to grow even further by 2025 (up to USD 6.2 trillion). The size of objects connected to the IoT varies from tiny computers of the size of a grain of dust to entire smart cities. The infographic also features new technologies such as smart locks and smart buildings, as well as expected technologies of the future (man-machine mind meld). This plethora of devices shows heterogeneous security needs and an evolving roadmap of application in a critical environment.

The threats and risks related to the IoT devices, systems, and services are numerous and at a constant rise. ENISA's Baseline Security Recommendations for IoT report [5] provides general security recommendations for IoT highlighting Critical Information Infrastructures, consisting of facilities, networks, services, and physical and IT equipment. By taking differences in allocating risks to different environments into consideration, the report provides an overview of a set of areas of IoT including smart homes, smart cities and intelligent public transport, smart grids, cars and airports, and eHealth and smart hospitals. Afterward, the report provides a thorough overview of IoT security practices, guidelines, existing industry standards, and research initiatives in the field of IoT security for Critical Information Infrastructure. Based on the findings, ENISA suggests baseline security measures. The report also focused on IoT resilience and communication, as well as on the interoperability with proprietary systems, reliability of IoT, and privacy issues related to smart infrastructure and services.

RFC 8576, entitled ”Internet of Things (IoT) Security: State of the Art and Challenges” [6], provides a more focused overview of critical security aspects related to the IoT. First, it discusses the topic of the lifecycle of a thing in the context, which applies to different IoT applications and scenarios. Afterward, it summarizes the security threats for IoT, as well as methodologies that can be used for coping with these threats. Moreover, it classifies threats into the following categories: i) Vulnerable software/code, ii) Privacy threat, iii) Cloning of things, iv) Malicious substitution of things, v) Eavesdropping attack, vi) A man-in-the-middle attack, vii) Firmware attacks, viii) Extraction of private information, ix) Routing attack, x) Elevation of privilege, xii) DoS attack. The approach is similar to other regulatory documents where specific attacks are considered as threats for the target. For dealing with the threats, the report suggests the following methodologies: i) Business Impact Analysis, ii) Risk Assessment, iii) Privacy Impact Assessment, iv) Procedures for incident reporting and mitigation. These methodologies are quite standard and applicable in any context. The report also reviews existing state-of-the-art IP-based protocols for the IoT, as well as existing guidelines and regulations. Finally, the report discusses the other challenges for a secure IoT and the potential solutions for them. Some of the discussed topics include resource constraints, operational challenges, privacy protection, reverse-engineering considerations, and trustworthy IoT operations among many others.

ITU-T Y.4806 security recommendation [7] provides a classification of security problems related to the Internet of Things and analyses how security threats can impact safety. Then, it determines which security features can support safe IoT deployment. The provided recommendations by this report are tailored to safety-critical Internet of Things systems, including industrial automation, automotive systems, transportation, smart cities, wearable, and standalone medical devices. However, it is stated that they do not have any restrictions, meaning that they can be applied to any domain in the field of the IoT. The report first takes into consideration the types of environments of which the IoT consists, i.e., the virtual and the physical environment. Based on these two environments, virtual (V) and physical (P), as well as the thing (T), the report discusses the potential impact vectors in the IoT. Then it provides a brief overview of threats relevant to each impact vector considering that it may i) take place only for the things presented both in the physical and virtual environment, ii) be caused remotely without physical access to the thing, iii) go beyond the Confidentiality, Integrity, Availability (CIA) aspects, iv) cause functional safety issues. Then, it scrutinizes a list of security capabilities including communication, data management, service provisioning, integration, authentication and authorization, and audit that can be used to establish safer and more secure IoT.

ETSI EN 303 645 - Cyber Security for Consumer Internet of Things: Baseline Requirements report [8] presents information security practices for IoT devices through the means of high-level outcome-focused provisions, to support developers and manufacturers of consumer IoT. The report focuses on the most essential technical controls and organizational policies for tackling the most common security flaws. To counteract elementary attacks on underlying design vulnerabilities, the report considers only a baseline security level that can be complemented by more specific standards, permitting simpler development of assurance schemes. The report also provides several recommendations to IoT device manufacturers for protecting personal data. These recommendations are related to data processing and the collection of telemetric data. The report suggests that customers should be informed on which and how personal data are being processed, should explicitly state their consent, and should withdraw their consent at any given time. Furthermore, if telemetry data are collected, their processing should be minimized and customers should be acknowledged which, how, and for which purpose telemetry data are being processed.

Even considering the heterogeneous nature of the assets belonging to the Device/IoT domain (e.g., smart cars [9], smart grid [10], smart homes [11]), the IETF definition of threat, namely, '*a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm*', is general enough to cover with all the IoT threats. IoT has a specific peculiarity: the strong link between security leakages and safety. ITU-T in its report Y.4806 underlines this link identifying a list of threats that are capable to affect safety. OWASP identifies its top 10 IoT security threats where the weakness of passwords, network services, and interfaces are identified as the top three threats.

CONCORDIA threat taxonomy is a consolidation of threats previously considered in other documents/reports [10, 11, 12] and is composed of the following category:

- TG1.1 – Unintentional damage/loss of information or IT assets: This group includes all threats causing unintentional damage including safety and information leakage or sharing due to human errors.
- TG1.2 – Interception and unauthorised acquisition: This group includes threats introduced by alteration/manipulation of the communications between two parties. This TG, depending on the circumstances of the incident, can also be linked to TG5.
- TG1.3 – Intentional physical damage: in IoT the physical access to the devices that are spread in a potential uncontrolled environment is more serious than in another domain.
- TG1.4 – Nefarious activity/abuse: This group includes threats coming from nefarious activities. It requires active attacks targeting the infrastructure of the victim, including the installation or use of malicious tools and software.

- TG1.5 – Legal: This group provides for threats resulting from violation of laws and/or regulations, such as the inappropriate use of Intellectual Property Rights, the misuse of personal data, the necessity to comply with judiciary decisions dictated with the rule of law. Chapter 8 of the present document will discuss aspects of this TG.
- TG1.6 – Organisational threats: This group includes threats to the organisational sphere.

3.1.2 Network-Centric Security

The GSMA mobile telecommunications report 2020 [13] reviews the current threat landscape and underlines the main threats and predicts the future growth of threats to the telecommunications industry. The report also provides recommendations for telecommunications operators on how to cope with threats using a holistic view on technology, processes and people. Moreover, the report divides threats into eight domains, namely:

- Supply Chain Resilience: Unknown threat, which should be managed via contractual controls regarding security and governance within supplier organisation and should start at ITT/RFI stage.
- Securing the 5G Era: The security implementations that 5G can deliver are yet to be realized. Alongside rollouts and 5G service launches, security has to be embedded to prevent potential threats before they get the chance of impacting the network.
- Software Threats: Almost a half (47%) of all released Operational Support Systems (OSS) components had a vulnerability in at least one of their dependencies in their latest versions.
- Signaling: Difficulty to replace legacy protocols and technology, which can be reduced by implementing technology at the right location and with appropriate rules and skillsets.
- Cloud and Virtualization: Outsourcing of service management without accountability, which can be solved by considering supply chain controls and data protection, and implementing secure deployment and management.
- Internet of Things: Consumer and Enterprise driven, it has to be managed by defining a secure lifecycle for devices and educating consumers regarding the threats to IoT devices.
- Security Skills Shortage: The broader security industry is facing a shortage of experienced cybersecurity personnel, and developing the required skills for protecting future and legacy networks poses a significant challenge.
- Securing Device Applications: Failure of updating the applications installed on devices can result in outdated privacy measures, which can ultimately lead to unauthorized use of consumer data.

Cloud Security Guide for SMEs report [14] by ENISA aims to assist Small and Medium Size Enterprises (SMEs) in understanding the network and information security risks and opportunities related to the use of cloud computing. ENISA Threat Landscape and Good Practice Guide for Internet Infrastructure report [12] scrutinizes threats related to Internet infrastructure and provides a list of guidelines to users and organisations to deal with them.

For several years now, vulnerable network assets have been exploited as preferred targets for cyberattacks. Malicious cyber actors often target network devices, and, once on the device, they can remain there undetected for long periods. After an incident, where administrators and security professionals perform forensic analysis and recover control, a malicious cyber actor with persistent access on network devices can reattack the recently cleaned hosts. The adoption of a security assurance process that covers the entire life cycle management starting from secure design, secure development, secure deployment, security monitoring, and security management is necessary to counteract these attacks. There are also cases where attackers do not need to compromise their intended target directly but can achieve their aim by compromising its supply chain where it is least secure. In the last years, there was an increase in breaches caused by vulnerable software. Any given software stack can contain many sources of components and libraries in differing versions, increasing the need to assess, test, and patch carefully. This threat highlights the importance of managing the supply chain.

Another source of well-known network breaches is the use of legacy protocols. Signaling exchange is required to establish and maintain a communication channel or session on telecommunication networks as well as allocate resources and manage networks. For example, 2/3G networks used Signaling System 7 (SS7) and SIGnalling Transport (SIGTRAN) while 4G relies on Diameter; all generations use Session IP (SIP) and GPRS Tunnel Protocol (GTP). Many fundamental services, such as short messaging service (SMS), are managed by these protocols. Many of these signaling protocols are outdated and have been implemented under a trust model that assumed well-behaved mobile operators without the need to deploy strong security controls.

Besides, another type of attack vector comes from a flaw in the specifications. The paper in [15] is an example of vulnerabilities discovered during a careful analysis of LTE access network protocol specifications and a demonstration of how those vulnerabilities can be exploited using open-source LTE software stack and low-cost hardware. The paper in [16] demonstrates instead the usefulness of adopting formal verification tools to automatically check whether the desired security properties are satisfied or if instead the defined protocols/procedures suffer from ambiguity or under-specification. To complete our overview of the attack scenario, another vector comes from the poor configuration of network nodes as highlighted in [17].

The most relevant network threats are reported according to the following categories [18, 19]:

- TG2.1: Unintentional damage/loss of information on IT assets: this group includes all threats causing unintentional information leakage or sharing due to human errors.
- TG2.2: Interception and unauthorised acquisition: this group includes any attack, passive or active, where the attacker attempts to listen, intercept or re-route traffic/data. A example is the man-in-the-middle attack. This group also includes manipulation attacks where the attacker attempts to alter or interfere with data in transit, in particular with signaling messages and routing information.
- TG2.3: Nefarious activity/abuse: this group includes threats coming from nefarious activities. It requires active attacks targeting the network infrastructure of the victim.
- TG2.4: Organisational threats: this group includes threats to the organisational sphere.

3.1.3 System-Centric Security

The ENISA study on the security aspects of virtualization report [20] provides an overview of the status of security of virtualized environments, as well as related issues and challenges, and best practices for safeguarding security in virtualized environments. The report uses a bottom-up approach and first elucidates the list of all security weaknesses (inspired by the MITRE CWE) related to virtualization, after which it groups up the identified weaknesses into vulnerability groups, before finally compiling the list threat groups with related vulnerability groups and weaknesses. The report also classifies different virtualization environments from Guest/Host OS to hypervisors and containers to align each group with the corresponding threats and good practices that should be used to mitigate the identified threats. Lastly, the report provides a gap analysis in which it highlights the areas where research and inquiries are required. Moreover, it analyses gaps in the areas of cryptography, privacy, multitenancy, isolation, resource management, roles and human resources, security assurance, forensics, and standards.

The Egregious 11' of the 2019 [21] surveyed industry experts on security issues in the cloud industry to rate 11 salient threats, risks, and vulnerabilities. The most prominent outcome is that compared to the previous CSA report, traditional cloud security issues under the responsibility of cloud service providers (CSPs), such as a Denial of Service, shared technology vulnerabilities and CSP data loss, and system vulnerabilities are no more ranked as important for the cloud user perspective. This suggests an increased maturity of the cloud user's understanding of the cloud, on one side, but should not lower the attention on such threats from the CSP perspective. It is interesting to note that the top threats reported are more in the area of potential control plane weaknesses and limited cloud visibility. Misconfiguration and inadequate change control, for instance, are ranked at position number two. Furthermore, misconfiguration is the leading cause of data breaches in the cloud. Also, the absence of automatic proactive change control is perceived as another risky weakness.

CONCORDIA's threat taxonomy is a consolidation of threats previously considered in other documents/reports and is composed of the following categories:

- TG3.1: Unintentional damage/loss of information or IT assets: This group includes all threats causing unintentional security leakage due to human errors.
- TG3.2: Interception and unauthorised acquisition: This group includes threats introduced by alteration/manipulation of the communications between two parties (including cloud internal communication channels). This TG, depending on the circumstances of the incident, could, also, be linked to TG3.5.
- TG3.3: Poisoning: This group includes all the threats due to configuration/business process poisoning and aiming to alter system behaviors (i.e., at any layers).
- TG3.4: Nefarious activity/abuse: This group includes threats coming from nefarious activities. It requires active attacks targeting the infrastructure at any layers like management hijacking and identity fraud.
- TG3.5: Legal: This group provides for threats resulting from violation of laws and/or regulations, such as the inappropriate use of Intellectual Property Rights, the misuse of personal data, the necessity to comply with judiciary decisions dictated with the rule of law. Chapter 8 of the present document will discuss aspects of this TG.
- TG3.6: Organisational threats: This group includes threats to the organisational sphere.

3.1.4 Data-Centric Security

The president of the European Commission Ursula von der Leyen wrote in her agenda that Europe had to develop joint standards for implementing 5G networks [22]. Today, 5G is a reality and Europe has to continue driving the standards already for 6G. To accomplish this goal, as well as other technological breakthroughs, technological sovereignty has to be achieved in several critical areas, and investments have to be increased in disruptive research and breakthrough innovation. The focus should be on the blockchain, high-performance computing, quantum computing, algorithms and tools for data sharing, and especially data and AI as two key ingredients for finding solutions to many societal challenges.

EU General Data Protection Regulation has already enabled flow and widespread use of data while safeguarding privacy, security, safety, and ethical standards. The Digital Services Act aims to improve liability and safety rules for platforms, services, and products while completing Digital Single Market. A Joint Cyber Unit should enable even faster information sharing and higher data privacy. Full digitalization of the European Commission will lead to the emergence of new work culture, fewer hierarchies, and better cooperation, which will help Europe to prepare for the future.

Digital businesses often generate data that can be more efficiently processed when computing power is in the vicinity of the source of data generation. To localize computing power, edge computing solutions can be used, which come with several perks and risks. By 2025, Gartner predicts that 75% of the enterprise-generated data will be created outside the centralized data server or clouds [23]. Edge computing solutions come in many forms, ranging from basic event filtering to complex-event processing and batch processing. They can be utilized in a large number of areas, such as health, e.g., health monitors that can measure the heart rate, traffic, where they can act as gateways and collect GPS signal or traffic signals data, 5G networks, oil rigs, and so on. The potential risks of edge computing solutions include security due to the increased attack surface (distributed Denial of Service attacks can target unsecured endpoints to access core networks), and scalability in terms of financial benefits.

According to ENISA Big Data Threat Landscape [24], a threat to a Big Data asset can be considered as '*any circumstance or event that affects, often simultaneously, big volumes of data and/or data in various sources and of various types and/or data of great value'. It can be further divided into Big Data breach when 'a digital information asset is stolen by attackers by breaking into the ICT systems or networks where it is held/transported' and Big Data Leak 'the (total or partial) accidental disclosure of a Big Data asset at a certain stage of its lifecycle [...] due to inadequate design, improper software adaptation or when a business process fails*'. A Big Data Breach involves a malicious attacker's behavior resulting in unauthorised access, while a Big Data Leak involves an honest-but-curious attacker or an observer.

CONCORDIA's threat taxonomy is a consolidation of threats previously considered in other documents/reports11 and is composed of the following category:

- TG4.1: Unintentional damage/loss of information or IT assets: This group includes all threats causing unintentional information leakage or sharing due to human errors.
- TG4.2: Interception and unauthorised acquisition: This group includes threats introduced by alteration/manipulation of the communications between two parties. This TG, depending on the circumstances of the incident, could, also, be linked to TG4.5.
- TG4.3: Poisoning: This group includes all threats due to data/model poisoning and aiming to picture a scenario that not adhere to reality.
- TG4.4: Nefarious activity/abuse: This group includes threats coming from nefarious activities. It requires active attacks targeting the infrastructure of the victim, including the installation or use of malicious tools and software.
- TG4.5: Legal: This group includes threats due to violation of laws or regulations, the breach of legislation, the failure to meet contractual requirements,

the unauthorised use of Intellectual Property resources, the abuse of personal data, the necessity to obey judiciary decisions and court orders. We will discuss all these issues in detail in Chapter 8.

- TG4.6: Organisational threats: This group includes threats to the organisational sphere.

3.1.5 Application-Centric Security

OWASP Top 10 report [25] identifies the top 10 web application security risks in 2017 as follows: i) Injection - SQL, NoSQL, OS, and LDAP injection security threats; ii) Broken Authentication - Incorrectly implemented authentications mechanisms leading to compromised user credentials; iii) Sensitive Data Exposure - Failure to adequately protect sensitive information, such as financial, healthcare, and PII; iv) XML External Entities (XXE) – Poor configuration of older XML processors potentially leading to internal files disclosure; v) Broken Access Control - Failure to properly enforce restrictions on authenticated users; vi) Security Misconfiguration – Result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information; vii) Cross-Site Scripting (XSS) – Result of inclusion of untrusted data in a new web page without required validation or escaping; viii) Insecure Decentralization – Flaw potentially leading to remote code execution or an array of the other potential attacks; ix) Using Components with Known Vulnerabilities – Exploitation of the vulnerable component can lead to the data loss or server hijacking, x) Insufficient Logging and Monitoring – Combined with missing/ineffective integration with incident response resulting in further attacks to systems and destruction of data. Besides identifying threats, OWASP reports also provide guidelines for developers, security testers, organisations, and application managers concerning the ways how to deal with the identified threats.

The CWE/SANS report [26] underlines the top 25 software errors that can lead to weaknesses in the software. Out of these 25 errors, the first ten include i) Improper Restriction of Operations within the Bounds of a Memory Buffer; ii) Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'); iii) Improper Input Validation; iv) Information Exposure; v) Out-of-bounds Read; vi) Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'); vii) Use After Free; viii) Integer Overflow or Wraparound; ix) Cross-Site Request Forgery (CSRF); x) Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'). To eliminate those errors, SANS researchers suggest undergoing through a number of the steps, including: i) SANS Application Security Courses; ii) Developer Security Awareness Training; iii) Using automated tools that test software for these errors; iv) Following procurement standards for buying secure software.

A threat to application assets can be considered as '*any circumstance or event that affects, often simultaneously, services and applications distributed over the*

Web'. The threat taxonomy is a consolidation of threats previously considered in other documents/reports such as related to OWASP Top 10, and CWE/SANS Top 25, mentioned above [25, 26] and is composed of the following categories:

- TG5.1: Unintentional damage: This group includes all threats causing application malfunctioning or loss of confidentiality/integrity/availability due to human errors.
- TG5.2: Interception and unauthorised acquisition: This group includes threats introduced by alteration/manipulation of the communications between two parties. This TG, depending on the circumstances of the incident, could, also, be linked to TG5.4.
- TG5.3: Nefarious activity/abuse: This group includes threats coming from nefarious activities. It requires active attacks targeting the platform of the victim, as well as public interfaces of the hosting platform and applications.
- TG5.4: Legal: This group provides for threats resulting from violations of laws and/or regulations, such as the inappropriate use of Intellectual Property Rights, the misuse of personal data, the necessity to comply with judiciary decisions dictated with the rule of law. Chapter 8 of the present document will discuss certain aspects of this TG identified.
- TG5.5: Organisational threats: This group includes threats to the organisational sphere.

3.1.6 User-Centric Security

In ISO/IEC 27001:2013 [27], requirements for establishing, implementing, maintaining, and continuously enhancing information security management systems within organisations are specified. Moreover, requirements for the assessment and treatment of information security risks are specified according to the organisations' needs. The specified requirements are universal and applicable to organisations of all types and sizes. Threats to information systems, including purposeful attacks, environmental disruptions, human errors, and structural failures are ubiquitous and can leave critical consequences on organisations, operations, and individuals. Hence, it is of the essence that information security risks are well understood and managed in the right way. Risk management is the essential part of an organisational risk management process, and its purpose is to identify relevant threats to organisations or threats directed through organisations against other organisations, internal and external vulnerabilities to organisations, the potential impact of threats, and the probability that harm will take place.

ENISA, Cybersecurity Culture in organisations report [28] discusses strategies for promoting and enhancing Cybersecurity Culture (CSC) in organisations by drawing from numerous disciplines, such as organisational sciences, psychology, law, and Cybersecurity, as well as with the knowledge and experience from the already existing CSC programs within organisations.

The NIST SP 800-30 report [29] provides guidance for conducting risk assessments of information systems and organisations. Risk assessments are proposed to be carried out on three tiers of the risk management hierarchy, including organisational level, mission/business process level, and information system level. Besides, NIST SP 800-30 provides a guideline on how risk assessments and other organisational management processes complain, as well as guidelines on identifying particular risk factors to be monitored continuously. This can help organisations in determining whether the risks have exceeded organisational risk tolerance, and changing courses of action if required.

Europol's Internet Organised Crime Threat Assessment (IOCTA) report [30] assessed the emerging cybercrime threats ad key developments for 2018. The report aimed to provide insights to law enforcement for fighting both persistent and the novel forms of cybercrime. The report came to several conclusions, including: i) Dominance of ransomware in 2018; ii) Continued production of Child Sexual Exploitation Material (CSEM); iii) Continuous use of DDoS attacks on public and private organisations; iv) Dominance of card-not-present fraud and persistence of skimming; v) Growth of cryptocurrencies' abuse targeting currency users and exchangers; vi) Social engineering is the engine of an array of cybercrimes; vii) Cryptojacking as a new cybercrime trend; viii) Perseverance of Darknet despite major blows taken by law enforcement. The report also underlined the following key findings: i) Ransomware was the main malware threat, and brute force, spam, and social engineering became the main methods of infection; ii) The amount of CSEM continued growing and targeting an increasing number of minors; iii) Telecommunications fraud established as a new challenge for law enforcement, while new payment fraud abuse methods, such as manipulation of devices emerged; iv) Number of smaller Darknet markets started growing; v) Despite continuing spreading propaganda, Islamic State (IS) started showing internal limitations; vi) Phishing, business email compromise, and traditional scams continued targeting an increasing number of victims, while the focus of financial cyberattacks moved to cryptocurrencies. Ultimately, the report provided specific recommendations for coping with each of the identified cybercrime types, and briefly described dissemination and cybercrime trends throughout different parts of the world.

A threat to user assets can be considered as '*any circumstance or event that produces adverse effects primarily on individuals as part of an organization or as stakeholders. The threat should be carried out through digital means, either voluntarily (attack/cybercrime) or involuntarily (human error)*'. The threat taxonomy is composed of the following categories:

- TG6.1: Human errors: This group includes all threats causing unintentional information leakage or sharing due to human errors.
- TG6.2: Privacy breaches: This group includes all threats causing privacy breaches.
- TG6.3: Cybercrime: This group includes all threats due to data/model poisoning and aiming to picture a scenario that does not adhere to reality.

- TG6.4: Media amplification effects: This group includes threats coming from nefarious activities. It requires active attacks targeting the infrastructure of the victim, including the installation or use of malicious tools and software (see Appendix A.6 for more details).
- TG6.5: Organisational threats: This group includes threats to the organisational sphere.

3.2 Cybersecurity Threat Map

Drawing upon the domains of interest, this section provides a Cybersecurity Threat Map that specifies for each of the identified threat groups the relevant threats in the domains network, system, device/IoT, data, application, and user.

From Table 2, where numbers in parenthesis are used for threat numbering in the form T(D).(TG).(T), it emerges that threats groups are horizontal to the different domains. Some differences do nevertheless exist due to the peculiarities of each area. Also, threats in the area of data and users are cross-domain because often data represent the target of an attack, while users are often seen both as a target and as a threat agent.

3.2.1 Cybersecurity Threat Map

TThe recent ENISA Threat Landscape (ETL) 2020 (published on 20 October 2020) highlighted that COVID-19 led the transformation of the digital environment resulting in an impact on to threat landscape. During the pandemic, cybercriminals have been seen advancing their capabilities, adapting quickly, and targeting relevant victim groups more effectively. The ETL report highlights important aspects and trends related to the threat landscape. Below we report just a few of them that were impacted by COVID-19:

- There will be a new norm during and after the COVID-19 pandemic that is even more dependent on a secure and reliable cyberspace.
- The number of fake online shopping websites and fraudulent online merchants reportedly has increased during the COVID-19 pandemic. From copycats of popular brands websites to fraudulent services that never deliver the merchandise, the coronavirus revealed weaknesses in the trust model used in online shopping.
- The number of cyberbullying and sextortion incidents also increased with the COVID-19 pandemic. The adoption of mobile technology and subscription to digital platforms makes younger generations more vulnerable to these types of threats.
- The number of phishing victims in the EU continues to grow with malicious actors using the COVID-19 theme to lure them in. COVID-19-themed attacks include messages carrying malicious file attachments and messages

Table 2: Cybersecurity Threat Map

Domain (D)	Threat Group (TG)	Threats (T)
Device/IoT (1)	Unintentional damage / loss of information or IT assets (1)	Information leakage/sharing due to human errors (1) Inadequate design and planning or incorrect adaptation (2)
	Interception and unauthorised acquisition (2)	Interception of information (1) Unauthorised acquisition of information (2)
	Intentional Physical Damage (3)	Device modification (1) Extraction of private information (2)
	Nefarious activity/abuse (4)	Identity fraud (1) Denial of service (2) Malicious code/software/activity (3) Misuse of assurance tools (4) Failures of business process (5) Code execution and injection (unsecure APIs) (6)
	Legal (5)	Violation of laws or regulations (1)
	Organisational threats (6)	Skill shortage (1)
Network (2)	Unintentional damage / loss of information or IT assets (1)	Erroneous use or administration of devices and systems (1)
	Interception and unauthorised acquisition (2)	Signaling traffic interception (1) Data session hijacking (2) Traffic eavesdropping (3) Traffic redirection (4)
	Nefarious activity/abuse (3)	Exploitation of software bugs (1) Manipulation of hardware and firmware (2) Malicious code/software/activity (3) Remote activities (execution) (4) Malicious code - Signaling amplification attacks (5)
	Organisational (failure malfunction) (4)	Failures of devices or systems (1) Supply chain (2) Software bug (3)
System (3)	Unintentional damage / loss of information or IT assets (1)	Information leakage/sharing due to human errors (1) Inadequate design and planning or incorrect adaptation (2)
	Interception and unauthorised acquisition (2)	Interception of information (1) Unauthorised acquisition of information (data breach) (2)
	Poisoning (3)	Configuration poisoning (1) Business process poisoning (2)
	Nefarious activity/abuse (4)	Identity fraud (1) Denial of service (2) Malicious code/software/activity (3) Generation and use of rogue certificates (4) Misuse of assurance tools (5) Failures of business process (6) Code execution and injection (unsecure APIs) (7)
	Legal (5)	Violation of laws or regulations (1)
	Organisational threats (6)	Skill shortage (1) Malicious Insider (2)
Data (4)	Unintentional damage / loss of information or IT assets (1)	Information leakage/sharing due to human errors (1) Inadequate design and planning or incorrect adaptation (2)
	Interception and unauthorised acquisition (2)	Interception of information (1) Unauthorised acquisition of information (data breach) (2)
	Poisoning (3)	Data poisoning (1) Model poisoning (2)
	Nefarious activity/abuse (4)	Identity fraud (1) Denial of service (2) Malicious code/software /activity (3) Generation and use of rogue certificates (4) Misuse of assurance tools (5) Failures of business process (6) Code execution and injection (unsecure APIs) (7)
	Legal (5)	Violation of laws or regulations (1)
	Organisational threats (6)	Skill shortage (1) Malicious insider (2)
Application (5)	Unintentional damage (1)	Security Misconfiguration (1)
	Interception and unauthorised acquisition (2)	Interception of information (1) Sensitive data exposure (2)
	Nefarious activity/abuse (3)	Broken authentication and access control (1) Denial of service (2) Code execution and injection (unsecure APIs) (3) Insufficient logging and monitoring (4) Untrusted composition (5)
	Legal (4)	Violation of laws or regulations (1)
	Organisational threats (5)	Malicious Insider (2)
User (6)	Human Errors (1)	Mishandling of physical assets (1) Misconfiguration of systems (2) Loss of CIA[1] on data assets (3) Legal, reputational, and financial cost (4)
	Privacy breaches (2)	Profiling and discriminatory practices (1) Illegal acquisition of information (2)
	Cybercrime (3)	Organized criminal groups' activity (1) State-sponsored organizations' activity (2) Malicious employees or partners' activity (3)
	Media amplification effects (4)	Misinformation/disinformation campaigns (1) Smearing campaigns/market manipulation (2) Social responsibility/ethics-related incidents (3)
	Organisational threats (5)	Skill shortage/undefined Cybersecurity curricula (1) Business misalignment/shift of priorities (2)

[1] Confidentiality, Integrity, Availability (CIA)

containing malicious links that redirect users to phishing sites or malware downloads.

- Business Email Compromise (BEC) and COVID-19-themed attacks are being used in cyber-scams resulting in the loss of millions of euros for EU citizens and corporations.

In this context, the COVID-19 pandemic has brought a significant increase in and worked as a multiplier of cyberattacks, which directly or indirectly involve threats to data. Trustworthy and robust data management is more critical than ever because COVID-19 has changed our normality accelerating the distribution of computation to homes and the 'periphery'. According to EUROPOL, the new normal after COVID-19 must '*protect your children, house, finances, and data now that confinement measures are starting to relax. Criminals are still looking for victims. [31]*' Shopping, working and learning are delivered online at a scale never seen before [32]. Criminals changed their behavior to take advantages of the pandemic (showing criminal opportunism), building on the uncertainty of the scenario and the difficulties in distinguishing between reliable and unreliable information [30]. COVID-19 worked as a multiplier of the effects of existing threats such as social engineering, Distributed Denial of Service (DDoS), ransomware, child sexual abuse material, to name just a few. More in deep, lockdown and smart working moved and distributed computation away from businesses data centers increasing the risks of loss and interception of information, data breaches, unauthorized acquisition of information, and in general malicious attacks. Data compromise become key to any attacks and is amplified by increasingly effective social engineering, which builds on the so-called cybercrime as a service (CaaS) where facilitators offer their knowledge on the dark web [30]. Phishing scams and malware experienced a peak during the pandemic period and adapted their activities to target users tired by the lockdown and restrictions to freedom. Attackers masqueraded their activities aiming to capture personal data by acting as providers of information about vaccines, medical supplies, and hand sanitizers, portals to apply for payment of government assistance, to name just a few. [33, 34, 35]

The problems businesses are experiencing are not only the protection of their customers from phishing and social engineering attacks aimed to leak and breach customer information, but also the problem of protecting those data usually confined within the organisations that are exiting boundaries [36]. For instance, weak videoconferencing systems may not filter out uninvited people causing conversation eavesdropping and hijacking. As another example, smart working is increasing the risk of Ransomware attacks '*due to a combination of weaker controls on home IT and a higher likelihood of users clicking on COVID-19 themed ransomware lure emails given levels of anxiety [37].* This scenario is radically changing the threat landscape due to four main aspects: i) COVID-19 pandemic as a new threat vector; ii) attack prevention and detection that can be less effective in the new communication practices introduced by COVID-19; iii) the need of security teams to manage attacks in unfamiliar conditions, and iv) the rise in the importance of staff education and awareness. Generally speaking, statistics show that COVID-19 had a major impact on financial and healthcare businesses [38, 39]. Remote working also had a substantial impact on attacks with an average cost of a data breach increased by 137,000$ (IBM), with a peak of attacks related to COVID-19 (e.g., scams increased by 400% in March 2020 – ReedSmith, 33,000 unemployment applicants were exposed to a data security breach - NBC).

IT security budget must be also redistributed to consider perimeter security, next-generation identity, and access controls, remote access, automation, security training, security for trusted third parties [40], all aspects that relate to the need of protecting data and data management platforms. PwC identifies three main actions to mitigate emerging COVID-related risks: secure their newly implemented remote working practices; ensure the continuity of critical security functions; counter opportunistic threats that may be looking to take advantage of the situation [41]. In this context, however, according to Statistica, the economic crises is expected to cause a cut in the cybersecurity to spend of 8% in 2020. [1]

In addition, in the network domain, COVID-19 pandemic has led to:

- A spike in cyber threats that exploit telework technologies and remote tools. There is general exploitation of applications used for teleworking applications, including video conferencing software and Voice over Internet Protocol (VoIP) conference call systems. Malicious cyber actors are looking for ways to exploit telework software vulnerabilities to obtain sensitive information, eavesdrop on conference calls or virtual meetings, or conduct other malicious activities. Malicious cyber actors may target communication tools (VoIP phones, video conferencing equipment, and cloud-based communications systems) to overload services and take them offline or eavesdrop on conference calls. Cyber actors have also used video-teleconferencing (VTC) hijacking to disrupt conferences by inserting pornographic images, hate images, or threatening language. Some telework software allows for remote desktop sharing, which is beneficial for collaboration and presentations; however, malicious cyber actors historically have compromised remote desktop applications and can use compromised systems to move into other shared applications.
- An impact on security operations (SOC) and processes due to the increased remote workforce, the disparate managed and unmanaged endpoints, and a change in network traffic baseline.

Also, it comes as no surprise that criminals have repeatedly tried to exploit the state of fear, uncertainty, and doubt that many individuals have and still are experiencing. The infamous FUD triple (fear, uncertainty, and doubt) that has been for a long time the main driver for cybersecurity investments, has made an unexpected

[1] Spending on cybersecurity worldwide from 2017 to 2020 (COVID-19 adjusted) (in billion U.S. dollars), https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/, accessed Dec 14, 2020

return with the coronavirus, as a common feeling in society. As it already happened in the past, in the aftermath of dramatic events or existential threats (e.g., wars, past pandemics, economic crises, insurrections, or disasters), there are scammers ready to profit from people in a state of distress, feeling threatened, worried for relatives and desperately looking for remedies or healing. It has been documented that physical and movement restrictions, closures of workplaces, and all the uncertainties that the COVID-19 has brought have produced a spike in depression symptoms and condition of psychological distress. [42, 43]

Cybercriminals have carried out a whole lot of well-known online scams during the pandemic months of 2020. None of them is surprising or present any novel features. It is the usual arsenal of phishing email campaigns, fake products, fraudulent advertising, and preposterous pseudoscientific theories. Google has organised an awareness campaigns trough the website,[2] where safety tips are given concerning the most likely scams and prudent online behavior. The categories of scam listed by Google are: Fake healthcare organisations; malicious web sites falsely offering personal protection items urgently sought by individuals (e.g., face masks, hands sanitation products, etc.); scammers presenting themselves as representatives of governmental agencies (e.g., the tax revenue office); false financial offerings directed to people suffering harsh economic conditions; false donation campaigns for humanitarian support. Europol has created a similar web page for COVID-19 shopping scams [44] and another more comprehensive about safety tips [45]. There, the overview of the intersection between COVID-19 and criminal activities is broadened concerning the few of Google's tips. Europol reports cover the increase of sex offending and online child abuse cases, the response of drug markets to the new conditions during physical restriction periods, the spread of counterfeits, and the spread of disinformation campaigns. A bleak scenario is the one emerging from the Europol reports, much worse than 'simple' online scams highlighted by Google. The European Commission took notice too of the increased threat level to European citizens due to scams and, through its Consumer Protection Cooperation Network (CPC) arm, published its own website dedicated to scams and rogue traders during the COVID-19 pandemic. [46]

3.3 Technology Stack-related Recommendations

In the following, we provide a set of recommendations emerging from the threat landscape analysis so far, and in no particular order.

R1 – Focus on persistent threats. Providers and users should be aware of traditional threats, like software bugs, malware, and DoS, which span all over the ICT domains, from OS to networking and applications. Thanks to the complexity of modern systems, old vulnerabilities can revive in the context of a new domain. System designers and users should not lower the attention on traditional threats

[2] https://safety.google/securitytips-covid19/, accessed Dec. 14, 2020

that may find different applications in modern systems, like DoS that is evolving towards targeting IoT environment, by for instance speeding up battery consumption, instead of inducing service failures. The main countermeasures are weakness point discovery, upgrading and patching outdated systems when possible, and when not monitor relevant measures (e.g., battery consumption) to infer the system health status.

R2 – Find a good trade-off between security level and domains peculiarities. As underlined by the CSA Security Guidance for Critical Areas of Focus in Cloud Computing v4.0, not all the domains need the same security countermeasures to deal with cybersecurity risks. Excess of countermeasures could be as problematic as the lack of them. Any countermeasures themselves may extend the attack surface and could produce performance reduction that in some scenarios increases the exposure to security risks. The incredible request for digital services facilitated DDoS since the systems were overwhelmed by rightful requests. A domain-specific security by design is strongly suggested.

R3 – Tailored security investments. Connected to recommendation R2, it is becoming fundamental to analyse security also from a strictly economic point of view, considering that often critically important systems or components have their investments in related security activities neglected. When the budget is preventing full security countermeasure application, such as in some IoT scenarios, specific design analysis is needed involving risk evaluation to tailor the application of the countermeasures.

R4 – Protection from insider threats. Insider threats are difficult to mitigate, both when access to critical information with high privileges is granted by software components and when access is granted to humans/employees. However, they are becoming more insidious especially in distributed and federated systems. It is becoming more important to apply strict and homogenous authorization policies and strategies to monitor insider behavior even across different (federated) access control systems.

R5 – Consider the deployment environment untrusted. Nowadays the deployment environment can dynamically change over time and the relative security peculiarities can change themselves. It is important to consider this scenario when security features depend on environmental conditions. For instance, in some IoT scenarios, the devices are physically accessible, and this may allow security bypass and serious insider threat attacks. It is important to consider environment peculiarities and the corresponding attacker capabilities.

R6 – Digital twins and possible safety impact. The pervasiveness of ICT in every sector is increasingly exacerbating the relation between security and safety, opening to more severe risks. Examples are UAV, IoT in medical and industrial scenarios. It is important to consider physical safety and digital twins implications while evaluating security risks.

R7 – Protect the user profiling capabilities. Nowadays, applications strongly rely on user profiling to provide an increased user experience. On the other hand, profiling is becoming a powerful weapon in the hands of an attacker, especially when connected to advanced ML capabilities. Given the business value of profiling, it is unfeasible to recommend avoiding user profiling, but it is fundamental to protect such data and mechanisms to gain them as primary assets.

R8 – Protect the AI models, engines, and data pipelines from manipulations. Powerful AI engines will constitute in the future a new target for an attacker having the objective to lead an entity to take a wrong decision. AI models tampering is the easiest way to obtain such malicious behavior. Even if AI models seem not to be sensible as such, they contain a lot of values and should be protected. On one side, data poisoning becomes a huge driver towards more complex attacks. On the other side, model poisoning aims to poison the source of training data to fake the learning algorithm in considering malicious behaviour as a normal one. In this context, attacks can occur at two different steps of the ML pipeline: the training step and the inference step.

It is strongly recommended to develop robust AI models and protect them at inference time. It is also strongly recommended to protect the models and data integrity, avoid fake data/model injection, and the access to the AI engine to the authorized entity only running intact models. It is also recommended the definition and adoption of hardening and penetration tools against AI.

R9 – Consider the networking peculiarities while designing system security. Nowadays, the networking layer is no more than just a utility. It increasingly relies on software and services that are now offered as features to the customers. Security peculiarities, as well as weaknesses, need to be considered more than in the past where the leakages were more on the protocol implementation than on the networking infrastructure. Software-Defined Networks (SDN) and Network Functions Virtualisation (NFV) technologies are moving the traditional network architecture built on specialised hardware and software to virtualized network functions. Any software vulnerability will become more significant in this context. The consequence is increased exposure to third-party suppliers and the importance of robust patch management procedures (e.g., the core network functions of the 5G network are underlined as critical). It is fundamental to consider the network as vulnerable as any other software and avoid to abstract from the fact that it is virtualized or not. It is important to i) implement essential perimeter security defences to protect the underlying networks from attack at the physical level, as well as at any virtual network layers that they cannot directly protect themselves, ii) ensure isolation between virtual networks, even if controlled by the same consumer. It is also a good practice to implement internal security controls and policies to prevent both modification of consumer networks and monitoring of traffic without approval.

R10 – Protect from wide-band network-based localized DDoS. Low latency of 5G could allow better coordination among zombies in a DDoS attack scenario. The capillary diffusion of devices enabled by 5G will allow, for instance, an attacker to focus on a specific area covered by a slice leading to a new generation of better localized DDoS. It is important to adopt geographically localized DDoS countermeasures.

R11 – Protect edge computing nodes and services. Security concerns are shifting from a powerful and protected (e.g., Cloud) environment to a less powerful and less protected one at the edge. The trend is to let edge nodes pre-process row data that in most of the cases are very sensible since not aggregated or obfuscated at the origin. It is therefore very important to protect the edge computing nodes and balance the protection with the capabilities, possibly considering the adoption of end-to-end protection strategies traversing the edge to directly transfer to the cloud.

R12 – Adoption of serverless computing. The current trend of offering serverless computation even at the networking level with MEC introduces the need to rethink the application structure. It is important to use serverless services that i) match compliance and governance obligations, ii) reduce or eliminate attack surface and/or network attack paths. These services should be configured correctly to provide the required security features. The users while using them, should rely more on application-code scanning and logging and less on server and network logs.

R13 – Protect against AI weaponized threats. The adoption of Artificial Intelligence and Machine Learning techniques can substantially expand the attack surface of every domain, permitting to discover of vulnerabilities both in software components and in business process logic. DeepLocker is an example of a proof-of-concept evasive attack powered by AI developed by IBM. AI can be also used to spear-phishing campaigns, with automated social engineering and improved customization to increase the attack success rates. No real effective countermeasures exist except the possibility to use the same technology to protect and detect malware and breaches.

R14 – Protection against deepfake. Differently from the past, attackers are targeting people's reputation to gain an advantage and to play a scam (e.g., artificial intelligence-generated voice deepfake). The cyber-security companies are coming up with more and better detection algorithms, but this seems not enough. Examples are emerging technologies helping video makers authenticate their videos and the addition of digital 'artifacts' into videos to conceal the patterns pixels for face detection. It is important to educate employees on how to spot deepfake and have automatic checks built into any processes for disbursing funds. It is also important to adopt the good practice of 'trust by verifying'.

R15 – Conscious use of Social Networks. Social media and social networks represent another insidious source of an emerging cybersecurity threat. It is largely used to grab information about a target or to replace humans interacting over social media. It is important to be aware of what was published and on social bots activities as well.

R16 – Deep understanding of layered architecture security. Current systems are based on several software layers, often including a virtualization layer and the security of the upper layers normally depends on the security of the lower ones. It is important to consider all the layers involved in the design phase for correct security implementation. Each layer can be affected by the weaknesses of traditional systems like specific OSs.

R17 – Sharing and multi-tenancy concerns. The current trend is to increase the level of sharing and the density of the multi-tenancy, exacerbating the impact of most of the threats especially the ones that aimed to lower the performance under a critical threshold, or focused on tenant escape. It is mandatory to assure security isolation between tenants and strategies to avoid resource consumption under specific thresholds. Additional good practices are i) use secure hypervisors and implement a patch management process, ii) configure hypervisors to isolate virtual machines from each other.

It is also important to implement internal processes and technical security controls to prevent admin/non-tenant access to running VMs or volatile memory.

R18 – Consider the Virtualization/Containment weakness. Specific threats for virtualization and containment are evolving from escape to cross-layer hijacking. In general, containment, isolation, and sandboxing mechanisms will expose vulnerabilities in the future and their exploitation is normally associated with a very high-risk score. It is needed to i) provide sufficient security capabilities at the virtualization layers to allow users to properly secure their assets, ii) defend the physical infrastructure and virtualization platforms from attacks or internal compromises, iii) use a secure-by-default configuration approach. More specifically, for containers, some good practices are i) use physical or virtual machines to provide container isolation, ii) group containers of the same security contexts on the same physical and/or virtual hosts, iii) Ensure that only approved and secure container images or code can be deployed, iv) secure the container orchestrator/manager, v) ensure strong authentication for containers and repositories.

R19 – Control misconfiguration issues and foster transparency. According to CSA, misconfigurations, inadequate controls, and, in general, lack of transparency will become increasingly problematic especially in complex layered environments. It is strongly needed a configuration verification via continuous audit.

R20 – Avoid shadow IT. Modern attacks are capable to exploit behavioural information via shadow IT, which is increasing due to the plethora of services that are becoming part of the daily activities of employees. These attacks constitute the modern business process compromise threats. There is a strong need for assurance tools to mitigate this behavioral-oriented threat and control the company shadow IT that is nowadays difficult to be blocked due to their web-based nature.

R21 – Monitoring of human errors. A human mistake is more likely than in the past possibly causing failures in machine-controlled processes, a broad category that includes cybersecurity incidents. The reason is in the frequent presence of human-machine interfaces in business processes, as well as in the increasing complexity of digital-physical interactions in workplaces. This issue is very complex to counteract. It is recommended to keep the procedures involving humans as simple as possible, avoid error-prone steps, tight schedule, and conflicting requirements between security and productivity. Besides, every business process that involves humans should be monitored to detect incidental errors.

R22 – Continuous awareness campaign and training. Skill shortage is becoming more critical since today single and not-expert users are directly involved in complex business processes and can influence them. Configuration errors are therefore increasing as never seen before, introducing a huge amount of new opportunities for cybercriminals to affect the CIA (Confidentiality, Integrity, Availability) properties of systems and users. This is even exacerbated when the architecture requires interdisciplinary competencies to be used, like in the case of a Big Data platform. It is strongly needed to have a continuous training campaign for employers to limit human errors due to non-adequate skills. Besides, in the cloud architecture, it is fundamental to understand the concept of shared responsibility and ensure to understand the capabilities offered by cloud providers as well as any security gaps and best practices.

R23 – Protect the CIA triad of data. The fundamental role assumed by data in every aspect of our life makes attacks that aim to data breach and leak increasing. Traditional attacks like phishing and (D)DoS are reviving a new boost and mainly target the CIA triad of data. Today, a data breach or leakage can become a new weapon in the cybercriminal's hands, which will increase the number of extortion attacks with the threat of GDPR penalties deriving from data disclosure. It is needed to protect the users from advanced phishing including spear phishing, raising awareness within the company, and using any phishing systems. It is also fundamental to monitor and adopt anti-malware approaches to prevent/remove malware and detect malicious behaviours indicating the presence of malware-based bots. Besides. it is needed to protect from data breaches using traditional protections like access controls, encryptions but also monitoring the system (including API) for exfiltration and unauthorized access. Standards exist to help establish good security and the proper use of encryption and key management techniques and processes. On the other hand, leverage the architecture to improve data security and do not rely completely on access controls and encryption. We also remark that if the system is layered it is needed to encrypt any underlying physical storage, if it is not yet encrypted at another level, to prevent data exposure during driver replacements. It is also important to isolate encryption from data-management functions to prevent unapproved access to customer data. If a cloud is involved, consider the use of Cloud Access Security Broker (CASB) to monitor data flowing into the system.

R24 – Protect from mobile and IoT malware. Mobile malware is growing exponentially since 2017, following the increase in the use of mobile systems, such as mobile banking that is overtaking online banking. In this context, it is quite likely that the growth and development of mobile malware targeting users and applications will be observed. It is needed to protect and monitor mobile devices and limit their use for no business purposes when possible. In the case of IoT, system monitoring can help reducing botnet establishment.

R25 – Adopt security-aware development pipelines. GDPR advocates for security by design. Nowadays some technologies can help in supporting this principle. It is needed to build security into the initial design process and the system development lifecycle and to consider the adoption of continuous deployment and automating security into the deployment pipeline (e.g., adopting the DevSecOps principle). Threat modeling, static, and dynamic application security testing should all be integrated, and fuzzing should be considered. Testing should be configured to test also concerns specific to cloud platforms (if involved), such as stored API credentials. It is recommended to use i) software-defined security to automate security controls and ii) event-driven security, when available, to automate detection and remediation of security issues. Besides, it is needed to segregate access to the management plane and provide developers the possibility of locking down production environments.

R26 – Consider the complexity of the deployment environment. Traditionally, the application deployment environment is considered quite stable. Nowadays the increase in platform complexity and the proliferation of many (third-party) libraries open the door to new attacks (e.g., privilege escalation, hijacking, arbitrary code execution) that threaten not only the platform itself but also the users relying on it. It is needed to consider third party security and adopt strategies to check for security vulnerabilities while involving them as platform features or while building the solution. It is also needed to monitor the behavior of the solution post-deployment to check for security issues derived by any changes to the deployment environment.

R27 – Consider the miniaturization of the services. The advent of microservice architecture has increased the revenue for enterprises and supported new businesses, at the same time neglecting non-functional properties such as security and privacy. Security strongly depends on how these microservices are organised together in application workflows. Their dynamicity as well as the complexity of the workflows need to be considered. It is recommended to use security features offered by orchestrators and to consider audit and certification as a means to deal with composition dynamicity.

R28 – Protect CPS devices. Cyber-physical systems have brought changes to several aspects of daily life, like in electrical power grids, oil and natural gas distribution, transportation systems, health-care devices, household appliances, and many more. As often is the case with emerging technologies, they are riddled with security vulnerabilities that could easily become threats to users and individuals. It is recommended to i) ensure devices can be patched and upgraded, ii) do not store static credentials on devices that could lead to compromise of the cloud application or infrastructure, iii) protect the startup/reboot phase and the device tampering, physical substitution, and cloning, iv) encrypt communications, v) use a secure data collection pipeline and sanitize data to prevent exploitation of the cloud application, vi) assume all API requests are hostile.

These recommendations, summarized in Table 3, can be timely structured in short-term, mid-term and long-term as visualized in Figure 4.

Table 3: Overview of technology stack-related recommendations

R#	Recommendations
R1	Focus on persistent threats
R2	Find a good trade-off between security level and domains peculiarities
R3	Tailored security investments
R4	Protection from insider threats
R5	Consider the deployment environment untrusted
R6	Digital twins and possible safety impact
R7	Protect the user profiling capabilities
R8	Protect the AI models, engines, and data pipelines from manipulations
R9	Consider the networking peculiarities while designing system security
R10	Protect from wide-band network-based localized DDoS
R11	Protect edge computing nodes and services
R12	Adoption of serverless computing
R13	Protect against AI weaponized threats
R14	Protection against deepfake
R15	Conscious use of Social Networks
R16	Deep understanding of layered architecture security
R17	Sharing and multi-tenancy concerns
R18	Consider the Virtualization/Containment weakness
R19	Control misconfiguration issues and foster transparency
R20	Avoid shadow IT
R21	Monitoring of human errors
R22	Continuous awareness campaign and training
R23	Protect the CIA triad of data
R24	Protect from mobile and IoT malware
R25	Adopt security-aware development pipelines
R26	Consider the complexity of the deployment environment
R27	Consider the miniaturization of the services
R28	Protect CPS devices

3.4 Conclusions

ICT systems permeate the entire society putting people at the center of ICT-enabled businesses and domains. Traditional distributed systems are complemented with novel paradigms and scenarios (e.g., cloud and edge computing), and integrated with a multitude of heterogeneous smart devices and sensors. This scenario with the rise of business digitalization points to an environment where cybersecurity becomes key for system integrity and business success and is fundamental to protect citizen's safety as well. Today, data-driven economy, where an unprecedented

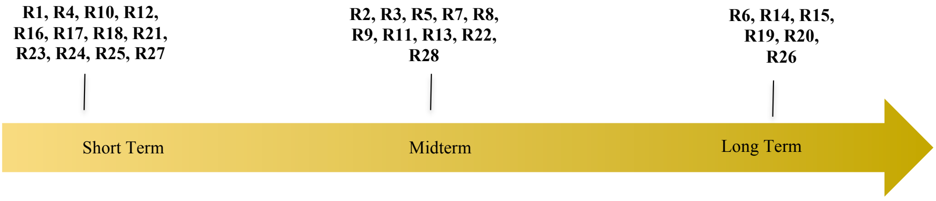


Figure 4: Overview from a technical perspective of most important directions, steps, and threats for short-, mid-, and long-term timelines

amount of data can be collected and analyzed, makes cybersecurity management even more critical than before introducing strong requirements on data and system protection, privacy and ethics, and safety protection. Also, the COVID-19 pandemic has worked as an amplifier of existing cybersecurity threats and challenges.

In this context, several recommendations emerge pointing to the primary need of managing increased digitalization in terms of increased user involvement and system complexity. Today ICT distributed systems are increasingly complex and difficult to manage, integrating diverse and heterogeneous technologies, from cloud to IoT, from 5G components to smart minuscule sensors, from Big Data to Artificial Intelligence platforms. These aspects coupled with an increasing lack of professional figures and expertise, especially in the data domain, make the problem of managing cybersecurity a difficult and error-prone activity. All these criticalities are further aggravated by the fact that people are becoming just another component of today's ICT distributed systems with all the risks introduced by the active involvement of people in a system working.

Data become central to system implementation, and data security represents a horizontal aspect impacting all domains of cybersecurity, while smart and targeted cyberattacks are increasingly on the rise (e.g., R1 and R6). Managing the impact of humans on cybersecurity is fundamental to reduce the risks of attacks and misconfiguration (e.g., R3, R4, R7). Appropriate training processes (R8), as well as tailored security investments (R9), are key to implement suitable countermeasures to cybersecurity attacks. The management of the system complexity is important to implement coherent and complete countermeasures that consider all aspects of the system (e.g., network, virtualization, services, cyber-physical systems) (e.g., R12, R13, R14, R20). New and targeted attacks must be addressed utilizing adaptive and flexible techniques (e.g., R23, R24). Last but not least, cybersecurity is today actively involved in protecting the final user of ICT systems and ICT-based services (e.g., R26, R27, R28).

4 Roadmap for Research and Innovation

As pointed out by Commissioner Breton, the digital sovereignty of Europe rests on three inseparable pillars: computing power, control over our data, and secure connectivity [47]. Computing power means that Europe should have the means to design and manufacture current and future computers, ranging from high-performance microprocessors [48] to quantum computers [49]. Control over our data means that European citizens should be able to trust that their data will be stored on cloud servers operating under EU law [50]. Secure connectivity means that data will be exchanged over a responsible Internet that increases the trust of our citizens [51].

In the next sections, we will identify some of the short-, mid-, and long-term research and innovation challenges we will be faced with. The focus hereby will be on challenges that are novel and therefore not (yet) sufficiently addressed by running EU activities. The results of this discussion will form the **Roadmap of Research and Innovation**, i.e., the technological roadmap.

CONCORDIA takes a holistic view on cybersecurity and identifies five layers, as known from the analysis of the threat landscape: i) device, ii) network, (iii) layer, (iv) data/application, and user's layer.

4.1 Device

The need to improve the security of devices is to a large extent motivated by the dramatic growth of the IoT. As part of their home automation, end-users will connect tens of billions of consumer devices to their Internet. To protect the privacy of these end-users and to avoid that these devices become part of a botnet, security awareness and measures should be strengthened. Less visible, but from a digital sovereignty point of view probably more important, are the devices that are embedded within cars, drones, and the devices that control our critical infrastructures and industrial systems.

To ensure Europe's digital sovereignty, Europe must keep its ability to develop its own hard- and software infrastructures.

In the past Europe always had a strong chip industry, and for the future, we should ensure that Europe remains the ability to design and manufacture its own high-performance microprocessors and other chips. In the next decades, we may expect that traditional computers will partially be replaced by quantum computers, which implies that Europe should strengthen its research in the area of quantum computers.

Traditionally, Europe has been strong in developing new devices such as mobile phones, as well as in developing software, including programming languages (such as Simula, Prolog, Pascal, Eiffel, Haskell, Python, PHP) and operating systems (Linux). However, for more recent developments, such as Artificial Intelligence (AI) and Machine Learning (ML), the European influence seems to diminish, despite some positive developments such as the European Laboratory for Learning and Intelligent System (ELLIS Society).

4.1.1 Transparency in the Software Supply Chain

To improve the security of devices, the software supply chain must become transparent. An enhanced level of transparency will also reinforce trust between the various parties and other relevant stakeholders. These notions have for instance been formulated by Allan Friedman, who is director of Cybersecurity Initiatives at the National Telecommunications and Information Administration at the US Department of Commerce. The problem with current device software is that it comes from many different sources, and even device developers do not oversee the origin or supply chain of the software that is included in the device.

Actions: To make the chain of components and their relationship transparent, a Software Bill of Materials should be included with each device. Such Bill of Materials can be expressed in terms of a Software Package Data Exchange (SPDX), as being developed by the SPDX workgroup of the Linux Foundation.

4.1.2 IoT Device Updates

Even if devices are tested and certified to be secure, and vulnerabilities will be discovered sooner or later. It is therefore important that each device includes facilities to be updated. To make such updating straightforward, current devices can be updated automatically over the air. For that purpose, consumer devices regularly contact servers at the vendor, to check if security updates are available.

A problem with this approach is that vendors can take over any device, by installing a prepared “security update”. Current approaches to update devices provide a backdoor to vendors and nation-states to take over devices. By taking control of such devices, vendors and nation-states can have the ability to spy on individual citizens and to misuse devices for large-scale attacks. This is particularly worrying since most IoT devices, or part of them, are not manufactured by European vendors.

Actions: To deal with this problem, all consumer devices must provide secure software update mechanisms. Besides, software updates should not only be triggered by the vendor, but they should also be certified. European researchers and regulators should therefore develop novel approaches and techniques to make such double certification possible.

4.1.3 Continuous re-certification with open hardware and software

The EU Cybersecurity Act aims to introduce for the first time an EU-wide security certification scheme for electronic devices. This presents unique challenges for research and industry. In the case of safety certification, a rigorous process of testing and documentation endows a high level of confidence that a device will behave as expected. In contrast, history has shown time and again that every complex software system contains exploitable vulnerabilities. Hundreds are discovered in the Linux kernel every year[3] .

In practice, security depends on our ability to issue software updates patches as soon as vulnerabilities are discovered. There are three basic building blocks required to automate this process on IoT devices, namely:

1. Digital certificates backed by a reliable PKI are needed to sign firmware images. For encrypted updates, digital certificates also provide the basis for end-to-end security between devices and update authors.
2. A trusted execution environment (TEE) on each device provides hardware-enforced isolation of security-critical software.
3. A small amount of trusted immutable code (i.e., the trusted computing base, or TCB) with exclusive access to the device hardware root of trust.

The TCB code executes in a TEE and is responsible for installing firmware updates on the device, and for providing the device owner with cryptographic proof that this has been done correctly – a process known as remote attestation. The advantage of this approach is that only the TCB and the hardware itself is fully trusted. The operating system and application code are complex and therefore likely to require security patches.

Actions: Ultimately, our objective is to create an automated re-certification solution, whereby devices can be issued with an EU-backed security certification that is valid until a vulnerability is discovered. When this occurs, devices must be patched and re-certified without any physical interaction. There are already ongoing efforts in the IETF SUIT working group to standardize the distribution of firmware updates and metadata[4]. One of the prime research focuses could be

[3] https://www.cvedetails.com/product/47/Linux-Linux-Kernel.html?vendor_id=33, accessed Dec. 14, 2020

[4] https://datatracker.ietf.org/group/suit/about/, accessed Dec 14, 2020

the implementation of TEEs on open-source RISC-V architectures that suits low-power IoT. With *automated* PKI, software updates, TEE, remote attestation, and dynamic AI-based code analysis, the vision of automated re-certification can become a reality.

4.1.4 Device identification and assessment mechanisms

Secure device identification is an essential step for establishing trust in a distributed computing environment. Being able to distinguish a clone from an expected genuine device is essential but not trivial. One approach is to design hardware components that can safely store device identity information (e.g., a device key) such that it is impossible to clone the stored information. The current trend is to make these hardware components more flexible and programmable, which will lead to a situation where the complexity of the security software grows to a point where its correctness the security software cannot be guaranteed any more. An alternative approach is to use physically unclonable properties of a device to establish the identity of the device.

Related to the identification of the device is the identification of the software components that are installed and/or running on a device. It is necessary to continuously assess the integrity of the software components and to detect attempts to compromise a device, including attacks exploiting so called zero-day vulnerabilities.

Device identification and assessment mechanisms need to be complemented by remote attestation protocols, which enable authorized third parties to assess the integrity of a device and its software and to detect changes. These protocols should be standardized, and the industry will benefit from openly available reference implementations.

Actions: Develop device identification mechanisms that exploit physically unclonable properties of devices. Develop novel techniques to continuously assess the integrity of installed and running software and that can detect deviations from expected normal control flows. Create standards and reference implementations of remote attestation protocols that enable applications to assess the identity and integrity of devices.

4.1.5 Embedded operating systems utilizing hardware security features

Hardware designed for embedded systems is nowadays being extended with special hardware security features that enable the separation of the execution of untrusted code running in a ”normal world” execution context from the execution of trusted code running in a ”secure world” execution context. Many new embedded operating systems have recently appeared but only a few exploit hardware security features to their full extend. While some embedded operating system projects are truly open source, others are driven by vendors promoting specific hardware designs. As embedded hardware becomes increasingly powerful, it will be useful to converge on a common embedded software framework that supports a larger number of embedded hardware designs. Hence, it is highly desirable to develop a common European open-source embedded operating systems utilizing hardware security features from the ground up. Ideally, this builds on existing expertise with open-source embedded operating system activities that are not controlled or driven by a single vendor.

Actions: Development of open-source embedded real-time operating systems that fully exploit hardware security features and that are not bound to vendor-specific and proprietary hardware solutions.

4.1.6 Microkernel isolation and virtualization mechanisms

In industrial environments and modern vehicles, the number of embedded control units is steadily increasing and reaching a point where consolidation is desirable since having separate embedded control units for each function is expensive and not scalable. Virtualization systems based on microkernel architectures start to become feasible and affordable for virtualizing embedded control units. However, more research needs to be done to achieve the level of isolation required for safety-critical functions. Besides, functions need to be integrated that can continuously measure the integrity and separation that is being achieved.

Actions: Development of light-weight virtualization mechanisms for embedded devices that provide isolation and resource control satisfying the requirements for virtualizing safety-critical functions.

4.1.7 Open-source secure processor and hardware designs

Critical infrastructures require trust in all software and hardware components. The availability of well-maintained open-source software has enabled the software industry to build software, including the software necessary to build software, from scratch using open-source components. On the hardware side, the industry typically relies on closed hardware designs and it has very limited tools at hand to verify whether a given piece of hardware is free from hidden functions or possible backdoors.

There is a movement towards open hardware designs. A prominent example at the processor level is the RISC-V project, providing an open-source CPU instruction set architecture enabling everybody to create RISC-V processors. Developing security extensions for RISC-V and hardware designs based on RISC-V technology will enable the industry to obtain hardware components from a variety of hardware components vendors, providing eventually the same control over the hardware components that are already possible on the software side.

Actions: Create an eco-system of open-source hardware designs enabling vendors to fully control the production of hardware components, which are used in products controlling critical infrastructures.

4.1.8 Postquantum Cryptography schemes on Constrained Devices

As quantum computers evolving to a real computational reality in the next few years, modern cryptography solutions (especially public-key cryptography) need to be reinvented to avoid quantum processor-based cryptanalysis that can lead to full disclosure of secrets in a reasonable amount of time. Thus, the cryptography research community in the past few years has invested time and effort to design and promote postquantum cryptography schemes that withstand quantum cryptanalytic attacks. NIST has launched a competition to award a standardized postquantum cryptography solution for Key Encapsulation Mechanisms (KEM) as well as Digital Signatures. The European research community has a prominent role in this process with several PQC (Post Quantum Cryptography) schemes reaching the final competition round. The competition will be concluded in the upcoming years and the winner schemes will be broadly adopted by the security community. However, when such schemes are transferred to the IoT environment and especially in resource-constrained end nodes, several implementation aspects need to be taken into account that is not originally included in the postquantum cryptography algorithm definition. The relatively big cryptography keys used by the PKE schemes as well as the computational complexity of those schemes may drain the resources of the existing IoT end node devices. The devices themselves may be deployed in a “hostile” environment where they may be attacked using side-channel attacks. Furthermore, security schemes for the IoT domain, like CoAPs do not take into account PQC solutions and further adaptation at the protocol level should be made (e.g., on TLS or DTLS).

Actions: The PQC solutions should be adapted to the IoT and Industrial IoT environment so that it can become deployable on resource-constrained devices. Also, PQC scheme implementations should be protected against side-channel attacks, including high order side-channel attacks. Existing IoT protocols that support security, should be adapted to the postquantum era by supporting PQC ciphers for KEM and digital signatures. Lightweight PQC scheme versions should also be researched and promoted to match the non-functional requirements of IoT end nodes and cyber-physical systems employed in the IoT/IIoT paradigm.

4.2 Network

Europe has an excellent track record in the area of networks. Europe has played a major role in the standardization and development of mobile networks, with companies such as Siemens, Alcatel-Lucent, Ericsson, and Nokia and the like. Technologies such as WiFi and Bluetooth were developed in Europe. Three of the largest Internet Exchanges are located in Europe (DE-CIX, AMS-IX, LINX), and connectivity for citizens and companies is world-class.

Europe is challenged, however, by the US and China (Huawei). If Europe loses control of its own networks, it runs the risk of becoming a digital colony of the US and/or China. Such development would not only have severe consequences for European companies (manufactures as well as operators), but ultimately our society and European values are at stake.

As Thierry Breton, the European Commissioner for the Internal Market already said, the digital sovereignty of Europe rests on three inseparable pillars: computing power, control over our data, and secure connectivity (=networks). Whereas major European programs already exist for computing (processors, quantum) and data (GAIA-X), a major program for networking seems to be missing. In this section, we will therefore identify some challenges to improve the security of European networks.

Probably Europe's biggest problem is that of fragmentation. Worldwide we witness a consolidation phase, where big companies take over smaller competitors. At this moment Europe has more than 50 mobile operators[5], of which only Deutsche Telekom, Telefonica, and Vodafone are within the top-ten[52]. The revenue of these three operators together is comparable to that of the biggest US operator (AT&T).

Because of this fragmentation, the security groups at most individual operators are relatively small and just able to follow the market. Real innovations often come from outside Europe, as is the case with DDoS protection services, DNS over HTTPS (DoH), and, more generally, the collection of network data that may be relevant for security.

A long-term solution for these problems would be the consolidation of smaller EU companies into bigger, more powerful companies. Due to the federated nature of Europe, such development would be politically extremely sensitive, and therefore not attainable in the short term. Fortunately, there are also many research and innovation actions that Europe could take now to strengthen its digital sovereignty and to ensure the security and privacy of its citizens.

One of the keys to all actions is to implement and monitor data sharing such as reflected in the Data Strategy of the Commission, and making infrastructures transparent. [6].

4.2.1 Open networking: The Responsible Internet

The problem of declining digital sovereignty is being addressed in several ways and different areas of technology, [51]. For example, Artificial Intelligence (AI) researchers have developed design guidelines to make the decisions of AI algorithms more transparent and explainable through what they call 'responsible AI'. Similarly, the European Commission is driving the development of a European federated cloud service called 'GAIA-X' that aims to improve Europe's data sovereignty.

[5] https://en.wikipedia.org/wiki/List_of_mobile_network_operators_of_Europe, accessed Dec 14, 2020

[6] Note: the term 5G security is sometimes used as an umbrella to denote the various steps that Europe needs to take to make its networks secure. The problem with such a term is that 5G is generally associated with mobile networks, leaving fiber and cable infrastructures aside. Besides, umbrella terms are generally not specific enough to identify the exact actions that need to be taken.

The European Commission recently also mapped out various policy instruments for areas such as 5G cellular access networks and the Internet of Things.

While these developments illustrate that digital sovereignty is a widely acknowledged and urgent problem, we observe the discussion largely overlooks the Internet infrastructure: the technical systems (e.g., routers, switches, and DNS servers) that enable remote internet devices to communicate with each other and that all of the other 'layers' (policy-making, AI, data) depend upon. The exception is the debate around the alleged security weaknesses in 5G equipment. According to the EC, these pose a risk to the strategic autonomy of the European Union, but 5G networks only cover the cellular access part of the internet infrastructure. The specific sovereignty problem in the Internet infrastructure is that users have no insight in, or control over how they depend on network operators and their systems, which ultimately poses a serious limitation for governments, institutions, companies, and individuals to decide how they can securely communicate. This is particularly relevant for critical service providers (e.g., power grids, transportation systems, mobile networks, and manufacturing facilities), which have become increasingly dependent on computer networks. For example, such providers want to know if the internet routes their traffic through networks with equipment that might have backdoors. At the same time, internet users by design depend on third parties because the Internet is a massively distributed and global system of some 70.000 autonomous networks. For example, during a typical website visit, users unknowingly make use of the services of several DNS operators, transit providers, cloud services, and content distribution providers, all of which may reside in different geographical locations and jurisdictions.

Actions: To fill this gap in the digital sovereignty discussion, we propose the notion of a **Responsible Internet**, a novel security-by-design extension of the Internet (or future networks) that offers users (e.g., providers of critical services or individuals) additional security-related options that give them a better grip on their dependencies on the internet, thus increasing their trust in and their sovereignty over internet communications. A Responsible Internet accomplishes this by making its networks more transparent, accountable, and controllable. This means users can ask a responsible internet to provide high-level descriptions of the chains of network operators (e.g., ISPs, data centers, and DNS operators) that potentially handle their data flows, for instance in terms of security and administrative properties, their interrelations, and the management operations they carried out (transparency). A Responsible Internet allows users to verify that these details are accurate (accountability) and to subsequently instruct the responsible infrastructure to handle their data flows in a specific way, for example by allowing them to only pass through network operators with certain verifiable security properties (controllability). The notion of a *responsible Internet* is inspired by *responsible AI*, a design paradigm that focuses on giving people more insight into how AI systems reach decisions and why

4.2.2 Trustworthy DNS resolver infrastructures

The DNS system takes care of translating domain names into IP addresses (e.g., `www.concordia-h2020.eu` – 139.91.90.171). Since DNS data provide a high-level overview of what network services exist and are used, DNS data is crucial for security purposes. However, in the absence of proper privacy protection rules, DNS data can also be misused to monitor the behavior of individual users. Fortunately, Europe has strong rules to protect the privacy of its citizens.

In the US such rules are lacking, and Internet providers are allowed to monitor the websites that their customers visit and sell that information to an advertisement and other companies. Since many customers do not like this, many US companies, most notably Google and Cloudflare, introduced the possibility to use DNS over HTTPS (DoH). By using DoH, Internet providers can no longer monitor the websites that their customers visit.

DoH is aggressively promoted by companies such as Google, and in the US browsers like Chrome and Firefox use DoH by default. However, migration towards DoH introduces the following problems:

- US companies like Google and Cloudflare collect even more data of European citizens,
- For European Security Operation Centres (SOCs) and national intelligence services it becomes harder or even impossible to detect security breaches,
- One of the most important Internet services, DNS, thus becomes under the control of a small number of (US) companies. This introduces vendor lock-in and potential single points of failure.

Actions: Although some aspects of DoH could potentially improve security, it is clear that changes are needed to solve the problems mentioned above. Research is therefore needed in the short term to address these challenges and make the necessary improvements.

4.2.3 DDoS protection Services

In a relatively short period, the Internet has become one of the, or probably the most important infrastructure(s) that our society relies upon. If the Internet would fail, airports, harbors, and shops should be closed, payment systems will fail, and working from home (in these times of COVID-19) becomes impossible.

In the last decade, we have witnessed an immense growth regarding the number as well as the strength of Distributed Denial of Service (DDoS) attacks on this vital infrastructure. Only five years ago most attacks were initiated by youngsters, spending a few Euros on a DDoS as a Service website (booter, stresser) to attack their favored bank. Fortunately, the mitigation of such attacks is relatively straightforward. Nowadays, however, we see ransomware attacks by criminals with strong technical skills on the Internet and Service Providers. These new attacks are quite challenging and therefore have the potential to disrupt parts of our society for longer periods.

To defend against DDoS attacks, many companies and organisations have outsourced their protection to Akamai, Cloudflare, and similar services. Although on average these DDoS protection services perform well, the fact that many of them are US-based creates new problems.

First, protection against layer 7 attacks often require that these companies should decrypt all data, including sensitive data such as medical health records and online payments. In principle, this gives Intelligence Services from outside the EU access to private information from EU-citizens. This is not only undesirable but might in some cases even be illegal.

Second, it creates a dependency on vital EU-services (such as healthcare end payments) on services from outside the EU. From the point of view of digital sovereignty, this is not what Europe should aim at.

Actions: It is important to further develop open and European approaches towards DDoS protection. The DDoS clearinghouse, as being developed within the EU CONCORDIA project, is a good first step. However, the focus of the DDoS clearinghouse is to share fingerprints of previous attacks, and not to protect against possible future attacks. Therefore, it is important to the extent the Clearinghouse with protection capabilities.

To cope with Terabit per second attacks, protection should be distributed over many locations, using technologies such as Anycast. In fact, a collaborative or federated protection architecture can be envisioned, in which similar services (for example banks or ISPs) share their DDoS protection capabilities to create a scalable DDoS protection service. More research on collaborative DDoS protection mechanisms is therefore needed now.

4.2.4 Monitoring and data collection infrastructure (data lakes)

The key to secure systems, services, and infrastructures, is the availability of data. Examples of data relevant for (network) security include DNS data, BGP data, location data, log files, traffic traces (pcap and flows), open ports, etc. Data is not only needed to detect future threats but also to understand trends. Data should therefore be stored for later analysis in so-called “data lakes”.

Every day the Internet is scanned by many parties. For example, criminals scan to find potential ransomware victims, nation-states scan to understand the state of the art, commercial organisations scan to share and sell data to interested customers. Examples of projects and organisations that scan the Internet include shodan.io, censys.io, RIPE Atlas, and OpenINTEL. But also passive data is important for security; examples include BGP data from Hurricane Electric, traffic traces from CAIDA, and security incidents by Shadowserver.

Actions: Europe should have the ability to collect, analyse, and archive the data that it considers important to secure its citizens and society. Of course, such activities should protect the privacy of its citizens by fulfilling the requirements of the GDPR, which means that critical analysis is always needed to decide which data is collected, and which not. Such analysis needs to be transparent for the general audience.

From a research perspective, the challenges include questions like:

- how to perform scanning in a scalable and privacy-sensitive way,
- how to quickly analyse huge data sets (big data analysis),
- how to correlate different and sometimes incompatible data sets (Machine Learning),
- how to condense and archive historical data, without losing precision, how to federate smaller data lakes to create bigger and therefore richer data lakes, without violating legislation or losing trust.

4.2.5 Network assurance & certification

The EU Cybersecurity Act introduces an EU-wide cybersecurity certification framework for ICT products, services, and processes to ensure security and trust in ICT systems, including mobile networks, across development, deployment, and operations. ENISA has a key role in setting up and maintaining European cybersecurity certification schemes. For instance, ENISA is currently considering adopting the GSMA/3GPP NESAS/SCAS [53, 54] certification scheme that has been jointly developed by GSMA and 3GPP for the certification of mobile networks equipment.

On the other hand, ICT technologies are developing at a fast pace and rapidly introduced in ICT systems, which in turn are increasingly being developed and released and deployed following the Continuous Integration & Continuous Deployment (CI/CD). However, Security Assurance Frameworks (SAF) have not evolved at the same pace as ICT systems:

- **Stasis** – SAF processes are defined for static targets with limited borders and features at a given point in time. Assurance for targets in development & operations is not sufficiently defined.
- **Slow and expensive** – SAF takes a long time to conduct with human-based evaluation work by skilled experts from various security fields in addition to the target's domain of application.
- **Inertia** – Upgrades or patches are either ignored or heavily delayed in domains with strict security SAF policies. Otherwise, vendors upgrade products but refer to outdated SAF proofs.
- **Waterfall** – SAF follows conventional waterfall process whereas ICT systems are engineered increasingly by Continuous Integration Continuous Deployment (CI/CD) practices.
- **Blurred targets** – SAF is equipment/device-oriented for bundled software and hardware. But ICT softwareization and virtualization decouples soft-

ware from infrastructure blurring the target's borders across software-, infrastructure- and service providers.

- **Technology (dis)trust** – There is a growing distrust on technology (origin) fearing backdoors in systems or components. It is not clear whether SAF can provide trustworthiness in this case.
- **Artificial Intelligence** – ICT systems are becoming AI-assisted. It is not clear how to evaluate AI unexplainable internals and its robustness against a new class of "intelligent" AI-based threats [55].

Actions: To enable an agile and trusted EU digital market, where the latest technology can be leveraged in ICT systems that in turn can be trusted based on evidence from agile security assurance frameworks, it is imperative to perform further research and foster innovation.

Short-term actions:

- **Metrics** – SAF should develop better quantitative metrics for measuring ICT trustworthiness.
- **Explainability** – SAF outcome is written for experts, but difficult to understand by stakeholders, not in the security field. Explainable and comprehensive assurance is needed for legal purposes, business decisions, and policymakers.
- **Automation & formal proofs** – SAF should leverage the latest advances in AI for automation of the assurance and re-assurance process to reduce the human-factor that is subject to subjectivisms or prone to errors. Automation is also an enabler towards formal proofs of assurance.

Long-term actions:

- **Embedded** – SAF should be agile and possible to embed in the ICT CI/CD lifecycle: development, deployment and operations. This would reduce the assessment and re-assessment burdens.
- **AI** – SAF shall include best practices end methodologies for evaluating the robustness of AI-based ICT systems that may contain bias or vulnerabilities against adversarial AI attacks.
- **Softwarization & Virtualization** – SAF should provide methodologies for assurance of virtualized and softwarized targets that are decoupled but still dependent on hardware and infrastructure.

4.3 System

Future research to improve the security of systems includes research on Quantum Technologies and Artificial Intelligence.

4.3.1 Quantum Technology

Quantum Technology (Q-tech). Q-tech is receiving high attention in research, industry, and governmental agencies. It is therefore important to outline an informed strategy based on a good understanding of the current status of the Q-tech and prioritize the right topics.

Based on existing research in Q-tech related initiatives [56] we can summarize the current status as follows:

- Quantum Computers – building a quantum computer is highly expensive and difficult. Its application is not general yet, i.e., it can efficiently solve a few specific problems (e.g., optimization problems).
- Quantum attacks on crypto – A recent report by experts from academia and industry judged that the construction during this decade of a quantum computer capable of breaking currently used public-key crypto would be highly unexpected. Symmetric crypto is quantum-safe, e.g., SIM card authentication. The business case for quantum adversaries is thus questionable. However, quite a lot of research and development is focused on post-quantum cryptography (sometimes referred to as quantum-proof, quantum-safe, or quantum-resistant).
- Quantum crypto – Evaluating and standardizing new crypto-systems necessarily takes time. The industrial benefits of quantum crypto are not directly applicable to all industries. Each industry sector needs to assess its suitability and feasibility.
- Quantum key distribution (QKD) – QKD is suitable in quantum communications and research shall remain in this quantum domain. QKD is primarily seen as a replacement of currently established key distribution protocols used for authentication, signatures, or integrity. Projects such as the EU H2020 project OPENQKD are building the EU's sensitive data and digital infrastructure for years to come.
- Governmental intelligence agencies – Based on authoritative sources, they are not in a hurry replacing commercially used public-key encryption.
- Quantum simulators – while useful in some domains, quantum simulation environments for cybersecurity purposes are questionable and no meaningful use case has been identified.
- Quantum Internet – The Quantum Internet is a network that will let quantum devices exchange information (Qubits) across a network with multiple quantum devices that are physically separated. The US Department of Energy [57] lays out a blueprint for the development of a national quantum Internet.

Actions: Based on the current state of the art and estimations about the expected progress the following research is needed:

- Open post-quantum crypto: Research in post-quantum crypto (aka quantum-safe) is of high-importance including wide and active participation in relevant standardization bodies such as IETF, NIST, 3GPP to ensure many-eyes expert reviews in an open transparent process. We need to avoid lock-in proprietary schemes taking over the market.
- Resilience: For industries relying on public-key cryptography (PKC), prepare risk-based recommendations on: i) develop post-quantum systems based on authoritative upcoming NIST standards; ii) prepare timed transition processes based on the progress of the authoritative research community; iii) prepare replacement, contingency, and containment strategies. For industries, this includes inventories of PKC-based protocols used (TLS, IPSec, S/MIME, SSH) and its base deployment in devices, appliances, networks, and services.

4.3.2 Adversarial Artificial Intelligence Attacks and Countermeasures

A very important aspect to be considered in AI usage for security purposes is the intrinsic vulnerability of AI data, algorithms, and models to adversarial AI attacks. This new attack surface can be considered hard to mitigate. AI adversarial attacks cannot be fixed since they rely on the learning nature and unavoidable use of data of an AI algorithm. AI technologies can be used as weapons for performing cybersecurity attacks by generating malicious traffic, malicious code as well as automating the hacking process. This weaponization of AI can be very potent since it is adaptable to the countermeasures provided by defenders. In parallel to this type of attack, data poisoning and model poisoning can also be performed to attack an existing AI infrastructure. These adversarial attacks on legit AI systems aim to render such systems blind to a specific type of inputs or reduce the AI systems' accuracy as a whole. The current threat landscape is very broad and has been identified as critical for the secure use of AI in European security and privacy sensitive domains (Law Enforcement, Health, Critical infrastructure domains, etc.). Also, it should be mentioned that there exists no well-structured detection framework that can assess vulnerabilities of AI systems against adversarial AI attacks or weaponized AIs. Given the growing usage of AI solutions, the need for such an assessment mechanism becomes great.

Actions: Acknowledging the potency of the above-mentioned attacks, agencies, organisations as well as industries across Europe should establish a "security net" for detection, response, and mitigation. The goal should be to create the means to: i) reduce the risk of attacks on AI systems, and ii) mitigate the impact of successful attacks.

AI adversarial attack protection (security net) can be structured in three layers, planning, implementation, and mitigation:

- **Planning:** At the design phase of an AI solution, including evaluation of possible training datasets as well as a choice of AI classifier and modeling algorithms, an AI risk assessment process could be formalized to perform ”AI Suitability Tests” that assess the risks of current and future application of AI datasets and algorithms. An acceptable level of AI use within a given application could be provided as an outcome. These tests should weigh the application’s vulnerability to attack, the consequence of an attack, and the availability of alternative AI-based methods.

Apart from the above, the AI risk assessment can also perform a formal validation of data collection practices and suggest mechanisms for protecting data and restricting data sharing to trusted entities only. Finally, in the planning layer, best practices should be extracted to manage the entire lifecycle of AI systems in the face of AI attacks. These practices apart from technical aspects they will include strategic, operational as well as legal/ethical aspects of AI deployment.

- **Implementation:** During this layer, the best practices should be further consolidated into adopted IT-related reforms on ATI solutions to make AI attacks more difficult to execute. The process relies heavily on setting up security/cybersecurity mechanisms that will protect the assets which are used to craft AI attacks, such as datasets and models e.g, by improving the cybersecurity of the systems on which these assets are stored. This includes installing cyber defense mechanisms that support the CIA triad and detect cyberattacks (intrusion detection, anomaly detection, etc.) using hardware and software means.
- **Mitigation:** Mitigating AI attacks is not an easy task since such attacks are advanced and have very recently appeared in the security domain. Existing research proposals should be extended to mature solutions. Detection and Mitigation techniques could rely on decreasing the success rates of backdoor (harder to identify and track) attacks also known as poisoning attacks (e.g., “pruning method”) but also techniques that introduce defense mechanisms (for detecting AI-based attacks) like Adversarial Training, Defensive Distillation, Generative Models and Regularization of datasets. The goal of the mitigation layer should be to:
  - Harden AI models to be resistant to fault data injection and poisoning attacks (during design).
  - Infuses the AI models with detection mechanisms so that they can classify (apart from valid data) also malicious data (during AI operation).
  - Record the cybersecurity incident related to the detected attacks and report it to the cybersecurity community.

Malware detection and analysis

Ransomware, and more generally malware encompassing a lot of other threats like spyware and botnets that weaken our digital systems. The surface of attacks of malware are broader and broader, it includes all IT infrastructures: computes, smartphones & tablets, IoT devices, cars, and industrial infrastructures. They are aimed at the ordinary citizen as well as companies and administrations, even hospitals. The design of these malicious codes is increasingly complex. That is why even old malware strains can be undetected, like recent Emotet attacks. The consequences are financially huge and can also lead to a malfunction of our critical infrastructures.

Actions: In this arms race, it is necessary to develop new malware defense concepts. A holistic approach that takes into account a broad set of information, is necessary. That said, there is also room for improvement to devise new cutting-edge anti-virus products by combining machine learning and formal methods along with system events augmentation.

Lastly, it is crucial to have access to a shared platform of malware collection and their related information.

Explainable Security Deep Analysis

Nowadays, ML approaches are more and more prominent as methods to analyse, classify, and then take action. This is quite well-known in systems like face recognition, but there are other applications like network traffic analysis or malware detection. In each case, it is important to be able to explain an analysis performed by AI systems and give reasons justifying actions taken (i.e., explainable AI). Thus, in forensics, proofs or attribution of an attack is a key issue, and so analysis should be returned enough explanations. Another field is one of the embedded systems. Decision systems in a car should be able to provide a reason for a decision.

Actions: In the domain of cyber-security, it is worth to develop Explainable Security Deep Analysis. This domain is already an important subject in AI, so we should have a closed loop in this direction.

Service Dependency Roadmap

The complexity and a plethora of services involved in distributed systems such as the Cloud entails significant and often manual work to understand the interconnection and the behavior of the services in the system. This hinders the profiling of threats and their propagation in the system. We plan to automate this process by using the capabilities of model checking that would essentially enable profiling and analysing the potential paths that could be taken by a threat to propagate in the system.

Actions: The midterm goal for the service dependency task is to develop techniques to perform automated multi-level threat detection in a large-scale data center or cloud systems. This inherently enables the cloud providers to assess the potential propagation paths of the threat and consequently, prioritize the services accordingly.

4.4 Data

To achieve digital sovereignty and increased levels of information technology security at the European level, it is important to identify research challenges that can act as enablers for the European industry to build the most secure products in the world (Security made in Europe). Here we present future research directions that are specific to data/application security.

4.4.1 EU-controlled Cloud Infrastructure (GAIA-X)

The EU aims to create GAIA-X, a secure and federated cloud European infrastructure that meets the highest standards of digital sovereignty by combining existing central and decentralized infrastructures. Consequently, common requirements derived from all European partners, openness, transparency, and use of secure, open technologies are important and will be used as foundations on which the framework aims to be built. It is thus necessary to provide access to secure, trustworthy and automated services and API-controlled infrastructures. Solutions must be able to minimize the leak/loss of data and increase security in software/applications development, to facilitate increased data value and support cross-sector cooperation.

4.4.2 Smart Technologies

The future of the facilitation of everyday life lies in smart technologies. Smart and green energy systems will generate electricity, store it, and interact with the power grid to provide the necessary energy. Smart health monitoring systems will provide care based on distributed data and intercommunication with other systems or actors (e.g., medical personnel). Smart commerce will facilitate international activities based on multiple types of data as well as numerous stakeholders. Hence, it becomes increasingly necessary to develop the means to manage and audit the security of such a system and continuously re-assess the security risk of the systems they form. The boundaries between end-user systems and infrastructure are increasingly blurring, raising the prospect of critical services being impacted by vulnerabilities at the edge. Increasingly, smart technologies embed various forms of intelligence, machine learning being the most common one amongst them. This enables us to adapt services to the current context and to create new ones. However, ML and AI also have new vulnerabilities that are as yet poorly understood. It is important to uncover and develop means of mitigating them. Best practices for interconnecting smart devices must include end-to-end security of an application and its communication with external services, data confidentiality/integrity/availability/anonymity, privacy controls over accessibility at different levels concerning actors and compliance with related assurance and certification standards.

4.4.3 Securing data/software in distributed computing environments

The IoT ecosystems are on the rise and with the imminent adoption of 5G, it will continue to grow, even more, creating multitudes of networks where data is being exchanged among and applications are executed on the different components. In this multi-device distributed environment, data can be used to provide integrity and trust among the communicating entities/running software, by securely identifying all involved parties. Operating systems driving such data/software, as well as the ability to securely update them, also play an important role in such environments. Thus, it is important to be able to provide solutions that secure this kind of data, their exchange, and the applications that depend upon them. We expect research in the future to tackle these important subjects as well.

4.4.4 Inter-networking in the future

Data flows through the Internet in massive amounts. However, users do not usually have a say in how their data is being processed and handled: who is responsible, where it is stored, in what format, under what security measures, etc. Furthermore, data can be intentionally mishandled or even used to launch cyberattacks (DDoS, phishing, etc.). It is important to provide security mechanisms that can assure the proper handling of data based on advertised security properties. Additionally, solutions need to provide users with the ability to verify that their data is being processed in the way they want.

4.5 User

To protect the security and privacy of European users, we concentrate in the first observation on three research challenges that are of eminent importance:

- Fighting disinformation in Europe
- Data ownership and Data Privacy
- Dynamic Attribute-Based Trusted Digital Identify Management

All challenges should be addressed to lead to short-, mid-and long-term research activities.

4.5.1 Fighting disinformation in Europe

Online social networks and online media platforms enable individuals from remote corners of the globe to share ideas, news, and opinions in an almost instantaneous manner. Social networks such as Twitter and Facebook have become a primary source of information for billions of users and the media where new cultural and political movements are formed and promoted. This high level of reliance on social media opened the field to malicious actors to pose new kinds of threats, which can have severe consequences at a societal level. Disinformation diffusion in social networks is one such threat carried out by diverse users who have various motives. For example, terrorist organisations deliberately diffuse false information for propaganda purposes, trying to inflict conflict or to cause extreme emotional reactions. Foreign interference of actors with motives against the EU using human or automated operated accounts (bots) can slander a candidate, trying to shift the outcome of national elections or impede the policy-making process in general.

Challenges:

- *Understanding the disinformation diffusion:* The multiplatform diffusion

  The mechanism, the channels, and dynamics of disinformation diffusion are neither clear nor easily assessable for analysis. The disinformation content can become viral following a complex path of transmission and through many online communication platforms. The disinformation content could first be originating in the ”periphery” of social platforms and become viral in mainstream media. QAnon conspiracy theory is such an example. It is a unified-conspiracy theory consisting of several other conspiracy theories such as Pizzagate. It originated on 4chan (by the anonymous user ”Q”) and then spread through multiple social media platforms.

- *Official malicious actors: Elected politicians:* Often, there is a symbiotic relationship between elected politicians and conspiracy theory promoters. Often, political parties are the source of disinformation – using as a tool the conspiracy theories aiming to create a political polarization which will consequently lead to a loyal political base. Hence, individuals who support reactionary and anti-scientific narratives can become part of the elected government. Although this is a mainly political challenge for the European democratic system, countermeasures against disinformation campaigns employed by the social platforms themselves could suppress political extremism.

Actions:

- *Early detection of disinformation:* Classify the content and identify the actors

  One of the main challenges is detecting disinformation and misinformation operations at an early stage – before becoming viral in the mainstream media. Therefore, research should be conducted on developing novel machine learning techniques that will classify the spread of information and identify the source of disinformation – the influential users who were responsible for the information diffusion.

- *Countering disinformation:* During crises such as the COVID-19 pandemic, false information such as pseudoscientific conspiracy theories can result in wide-spread panic and chaos. Hence, not only early detection but also countering the disinformation is crucially important. Conspiracy theories related to the origin of COVID-19 and the anti-vaccine movements could play a negative role in the fight against the pandemic. Therefore, it is crucial to develop countermeasures against conspiracy theories that will be, at the same time, in line with the democratic values of Europe, such as the freedom of speech. Research on the early identification of malicious users that lead to their suspension from the social platforms is one such direction. Also, it is not enough to suspend accounts spreading disinformation. It is of paramount importance to research social media dissemination strategies that increase the influence of correct fact-checking information by employing graph-theoretical, game-theoretical, and human factor principles.

- *Coordination – European disinformation observatories:* An integrated or federated European observatory of disinformation that will monitor the social media streams and disclose disinformation activities should be a long-term. The observatories are currently being established in any European country to form an internal interconnected network of national institutions. Each network hub collaborates with national authorities, fact-checking organisations, and research institutions. Research on how to properly share and aggregate information from multiple observatories could prove highly beneficial in the observatory integration effort.
- *Detection and Mitigation of Social Bots, resp. the Social Bot Pandemic:* Social bots are a long studied, yet unsolved problem in the online social ecosystem. Detection is still a key challenge. Adversarial machine learning is a promising approach to be used in the fight against all forms of online manipulation. Deepfakes and other recent advances in AI can support the identification of social bots.

4.5.2 Data Ownership and Data Privacy

The initial design requirements of the Internet and the Web in the early 60s and 90s were far different than those of today (i.e., connecting servers between academia, sharing content through simple websites, email exchange, etc.). Today, both the Internet and the Web have managed to exhibit tremendous evolvability and extendibility. They have succeeded in supporting services (e-commerce, e-banking, content distribution, video streaming, Web conferencing, etc.) and capabilities (broadband connection, mobility, satellite, etc.) that could hardly be imagined.

Online advertising and marketing appeared soon after the Web's appearance in the 90s and grew into an entire industry that is currently funding a large part of the so-called free services of the Internet. Advanced versions of web advertising and recommendation systems, in general, are heavily based on detailed personal data collected online from millions of individuals to offer tailored ad impressions and recommendations to maximize profits of the so-called ”Tech Companies,” such as Google, etc. Of course, the uncontrolled user tracking and personal data collection of individuals lead to data protection and privacy problems that have challenged the Internet and the Web today.

Actions: New research efforts are required to mitigate and control the challenges mentioned above. Below we identify different directions that we need to turn to our attention:

- *Data protection regulations:* In recent years, we have witnessed new data protection regulations such as the GDPR in Europe and the California Consumers Act in the US, to name some. Since new regulations are now in place, the challenge now is shifted towards how we can apply them in practice by proactively monitoring and detecting violations in an automated way. As a result, new tools and methodologies need to be implemented to automate such regulations' enforcement. Some examples include tools related to web tracking and personal data leakage detection, website classification to identify sensitive content websites as defined by GDPR and similar legislation, Cookie consent (opt-out) automation and monitoring, browser fingerprinting mitigation, personal data handling, storage, and localization monitoring, etc.
- *Personal data ownership:* New research needs to be conducted to allow users to have full control of their data, including their browsing patterns, shopping activities, social network activities, etc. The main focus of such tools should be but not limited to the following functionalities:
  - Data portability: Data owners should be able to move their data across different online services of their choice (i.e., move financial data from one online banking service to another). As a result, new research should be focusing on novel portable data structures and mechanisms to allow the above functionality.
  - Right to be forgotten: Data owners should be able to block access and delete their personal data across different online services (i.e., remove their data from a social network). New tools and methodologies need to be invented to ensure that personal data collected and stored online are under the full control of the data owner (users), rather than the data collector (online service), which is the current state that we are facing today.
  - Furthermore, we need to provide technologies and tools to allow users to benefit from their personal data (i.e., create new monetization schemes based on personal data sharing).
- *Personal data value and Human-Centric Data economy:* Most online services utilize personal data to increase their profits. For example, e-commerce websites can use personal data to train machine learning algorithms to optimize their inventory and product recommendations. The ad industry uses personal data at a massive scale to serve targeted and re-targeted advertisements at a higher premium, etc. In all the above scenarios, the data producer

(user) is only compensated by getting access to the corresponding online service for free in exchange for being tracked. Instead, it would be fairer for end-users to have direct financial benefits for their data. To provide economic benefits based on personal data, the following research questions need to be answered: What is the actual value of personal data? How can we estimate such value? What factors influence data value based on how data consumers use them? Based on what frameworks do the data owner and data user value them?

- *Personal Information Management Systems (PIMS):* A more recent trend towards addressing privacy and cybersecurity threats around personal data is introducing an additional entity between online services and end-users. The so-called Personal Information Management Systems (PIMS) or Data Vaults. Towards that direction, we need to investigate different paradigms, such as centralized vs. decentralized PIMS, distributed open source or centralized closed source approach, and what the pros and cons of each paradigm are to achieve adaptability and global acceptance. Besides, we need to identify what the critical parts of such an ambitious approach are (i.e., data integrity, trust between nodes, data access control, etc.)

4.5.3 Dynamic Attribute-Based Trusted Digital Identity Management

Data structured at a contextual-appropriate level of abstraction, an attribute, can be a very powerful means and an asset to contribute to digital trust. Especially, if these attributes are dynamic, these can constitute part of a digital pulse and another unique identifier. With that, it has a strong digital identity, authentication, and authorization capabilities that are needed in this Digital Age. Having a trusted and trustworthy digital identity is essential. Without a ‘strong’ digital identity, and without being able to authenticate both the identity of a person, the identity of organisations, and the identity of the persona and related mandate of the person within the organisation (‘authorization’), digitising systems and building, achieving and sustaining digital sovereignty will not be very successful.

Authentication and authorization are security challenges that need to be factored in given that the digitalisation of our societal, economic, governmental, and other systems within the European Union will result in the creation of digital identities of the relevant stakeholders that need to be safeguarded. With the increasing number of risks such as identity-related fraud and mass data breaches, people are becoming more and more hesitant to trust these systems and organisations, whether public or private sector, with their data. Therefore, the digitalisation processes in this digital age will have to establish a higher threshold when it comes to authenticating and authorizing the identities of the relevant persona.

As a basic standard, users must be authenticated and authorized access to their digital identity using multi-factor authentication (MFA) and is in scope and compliant to the eIDAS Directive, for instance, taking inspiration from the guidelines regarding the implementation of secure authentication such as established by FIGI

(Financial Inclusion Global Initiative), and the like. Such and similar (and preferably post-quantum proof) identity, authentication, and authorisation are needed based on the principles such as user-centric design, dynamic, and risk-based continuous authentication, a fine-grained authorisation that is serving both the private and public sector across all vertical industries and cross-border.

4.6 Roadmap for Research and Innovation

It is expected that certain recommendations and other details will be incorporated more extensively in the next edition of the Roadmap for Research and Innovation. The visualized current roadmap for research and innovation is shown in Figure 5.

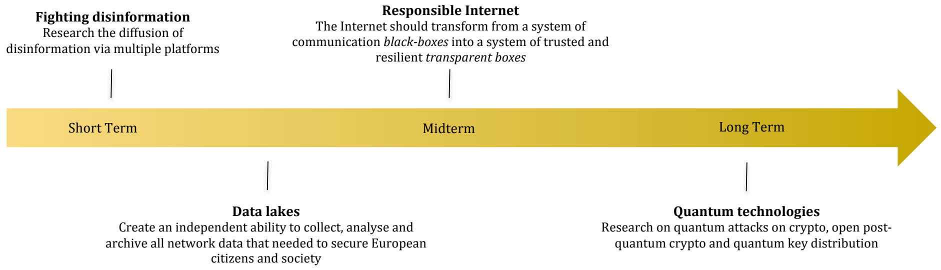

Fighting disinformation
Research the diffusion of disinformation via multiple platforms
Responsible Internet
The Internet should transform from a system of communication *black-boxes* into a system of trusted and resilient *transparent boxes*
Short Term
Midterm
Long Term
Data lakes
Create an independent ability to collect, analyse and archive all network data that needed to secure European citizens and society
Quantum technologies
Research on quantum attacks on crypto, open post-quantum crypto and quantum key distribution

Figure 5: Overview from a Research & Innovation perspective of most important directions, steps, and threats for short-, mid-, and long-term

5 Roadmap for Education and Skills

Cybersecurity as a concept in an industrial and business environment was considered in the past as an after-thought of the design and operation of the Informational Technology systems process. This had to do with the lack of proper training and security awareness of the business/industrial professionals involved in such environments. In the light of many cybersecurity attacks that have sometimes caused disorder at the European and international level and produced considerable risks and damages, this attitude has considerably changed. Besides, industry surveys reveal an increased interest in Cybersecurity awareness courses as an untrained staff is the greatest cyber risk to the business.

The challenges mentioned in the next chapter are based on our findings when assessing CONCORDIA's courses portfolio [58]. The recommendations listed below aim at answering to but also complementing some of the actions put forward by the European Commission in the Digital Education Action Plan (2021-2027) in both:

- Strategic priority 1 – Fostering the development of a high-performing digital education ecosystem
- Strategic priority 2 – Enhancing digital skills and competences for the digital transformation

5.1 Education for Professionals – Challenges and Recommendations

5.1.1 Challenges

C1. Skills gap

65% of kids today will do jobs that have not yet been invented[7]. Building up and enhancing skills is the most important attribute for both resilience and success in this dynamic, Digital Age. To prepare for tomorrow and beyond, we further need to both acknowledge that necessary skills in the era are, as also stated by OECD research [59], social skills, IT skills, science, technology, engineering and mathematics skills and self-organisation skills. This also, as jobs are expected to be lost due to automation, where it is expected that 80% of the current jobs will be seriously impacted, where about 14% will be lost due to automation within the next 15 years [59].

The World Economic Forum recently noted that 50% of all employees will need reskilling by 2025 as per adoption of technology increases, and critical thinking and problem-solving top the list of skills that people, organisation, and governments need to work on the next five years [59]. This brings tremendous opportunities for this cybersecurity and related domains, where there is an increasing need for skills, capabilities, and competencies, and a disproportionate amount of job vacancies. Currently, we do not have enough cybersecurity professionals to

[7] https://tinyurl.com/oecd-eductation-report, accessed Dec. 23, 2020

keep our vast and vulnerable digital and cyber-physical ecosystems safe, let alone build these, or being able to achieve and sustain digital sovereignty.

While the demand for security professionals continues to grow, the number of people with the skills and experience required for the job is not keeping pace[60]. Besides, the set of skills are changing as the cybersecurity professionals are expected to have a broader view of the company development, playing a more strategic role, and also include soft skills. This trend makes it more difficult to find and hire security professionals than a few years ago. The demand for cybersecurity professionals in 2020 was estimated will reach 1.5 million and is expected to double by 2021 [61]. By 2022 the security industry will most likely face a shortage of close to 2 million qualified personnel [62]. The shortage of skills is not only observed in professionals but also in teachers and lecturers. The main reason is that many of them either lack the industry experience or have not been involved in ”on-field” projects for a long time. The cyber domain is changing fast, so the people involved in training/education must closely monitor the field and collect as much experience from the real world as possible.

C2. Difficult to see the trainings big picture

Nowadays, there is a growing need by the industrial professional community for learning basic but also advanced Cybersecurity concepts. This is reflected in the considerable amount of offered Cybersecurity courses by various European and international organisations. However, despite the plethora of options to learn there is a profound lack of coherency and holistic planning in this training and awareness effort since each offered course (or series of courses) is designed based on different criteria from other courses (by another organisation). Hence, in several cases, this approach is confusing the trainee on what and how he should perceive cybersecurity concepts, as well as how to use them to cover his professional needs.

The lack of proper planning is also evidenced by the existing approaches to address the overall skills shortage in cybersecurity. Such approaches are more like short-term “patches” instead of a long-term carefully planned strategy. Universities add cybersecurity degrees to their curricula as a “specialization” to a Computer Science or Information Security degree and do not take into consideration the interdisciplinary nature of the field. In the business world, cybersecurity training occasionally falls victim to the high costs associated with it. The return on investment for cybersecurity tools and training is usually difficult to justify for the management and administration [63]. At the same time companies offering cybersecurity education and training, have to deal with customers that want to pay less for more value. People do not seem to understand how expensive it is to create and constantly update high-quality services in such a complex, dynamic, and interdisciplinary field.

C3. No EU Cybersecurity Skills Framework

Currently, there is no agreed EU cybersecurity skills framework. Efforts are made by ENISA that set up an ad-hoc working group to deal with this topic. In parallel, EU funded projects such as SPARTA are allocating resources to develop such a framework and start piloting it in few countries. CONCORDIA believes that an EU Cybersecurity Skills Framework would help in shaping specific academic and post-academic educational pathways as support for a career path in cybersecurity.

C4. Heterogeneity of competencies related terminology

The lack of a cross-domain and cross-industry agreed terminology related to the cybersecurity skills needed for a specific job makes it difficult for companies to fill in open positions. They find it hard to match the recruitment criteria with the studies and the qualifications listed in the CVs of the applicants because of the use of non-standard terminology. Individuals, in turn, cannot easily identify the skills they need to possess or develop to match market demand. And, finally, course providers have difficulties in designing curricula that answer to the market's needs.

C5: Cyber-attacks threaten all industries

Cyberattacks are threatening an increasing range of industries, thus changing the skills needed to perform traditional tasks. The extreme shortage of skills, the complexity of the field, and the associated costs make cybersecurity specialists an increasingly expensive profession, which only large companies and organisations can afford. The rest of the digital world (smaller companies, public organisations, etc.) operating on limited resources and employees with little or no background in cybersecurity, is left in a perilous position. For instance, physicians cannot simply take care of the patients but also need to protect their data. The same goes for lawyers who do not only need to understand the cybersecurity field if being a cybersecurity lawyer but also to protect the information they are working with as a significant amount of data is collected during the process. Moreover, the rapid evolution of IT technologies and devices used by the industry (e.g. IoT, digital economy, automation, etc.) and employees (e.g., personal mobiles, wearables, etc.) increase the attack surface and outstrip the skilled employees required to defend them [61].

C6. Cybersecurity is not only about technology

Among the main challenges of cybersecurity is the interdisciplinarity of the field [64] which cannot be addressed by just adding another responsibility to IT workers. Cybersecurity is not only computer science and IT, but also requires good knowledge of the law, social sciences, human factors/psychology, mathematics/ cryptography, economics, business planning, etc. It has become a board-level issue, a business risk; hence middle managers and executives would need to have an understanding of the importance of the topic and the economic impact of different decisions taken in this respect. Elements linked to business economics need to be considered as cybersecurity goes beyond technology and needs to be placed in the broader business context, e.g., when deciding on the investment priorities.

C7. Different level of cybersecurity preparedness

There is a different level of cybersecurity preparedness from the EU countries level, to individual companies' level, from big to small. Already in 2017, the Commission suggested that the main reason why some member states were more capable to establish CERTs than others was a 'cybersecurity skills gap' throughout the EU.

When it comes to organisations, it was estimated that more than 40% of cyber-attacks are targeting small businesses, 60% of them go out of business within six months of a cyber-attack. The skills shortage led to an increase in salaries, making it challenging for small organisations to attract talent to protect their organisation. Independent of their size, the companies' awareness and responsiveness to cybersecurity will condition their training strategy. Many are late to consider it a business need and therefore a Learning & Development issue to be considered and addressed, and usually leading to training of existing employees.

C8. Lack of cybersecurity culture

The lack of an established cybersecurity culture can be observed across multiple levels (technological, business, economic, societal, etc.). This directly affects existing professionals and people that want to get involved in cybersecurity. The main problem is the lack of clear career paths and development opportunities. Cybersecurity is still not viewed as a clear career path but a complementary skill to other IT jobs. For example, the World Economic Forum in its report for "Jobs of Tomorrow" [65], identifies cybersecurity as a Tech Disruptive Skill, but it does not include it as a profession in its list of growing job opportunities. People leaving the industry, indicate as reasons for this behaviour the lack of direction, burnout, and a toxic culture that can include discrimination or harassment. Moreover, the cybersecurity sector is suffering from a massive gender gap. Worldwide only 11% of its employees are women[8], value decreasing to 8% in Europe, and many of them have reported that they are often experiencing discrimination and some level of harassment[62].

C9. COVID-19 impacting the digital world

The COVID-19 pandemic brought cybersecurity under the spotlight. The shift to digital life of different age-categories of people and professions increased the cybersecurity-related risks thus the need to become knowledgeable on how to deal with them, according to their level of knowledge, usage of online services, and access to information.

[8] https://iamcybersafe.org/WomenInCybersecurity, accessed Dec 14, 2020

5.1.2 Recommendations

Based on the analysis so far, the following recommendations are formulated.

R1 - Mapping: one single map

- Who: EU institutions
- Relevance: EU level, course providers, companies, individuals
- One single website hosting all the existing Cybersecurity related programs (HEI, Ph.D., short courses for professionals). It will help an individual to identify the career path they want to follow, will help the content providers to benchmark their existing offer while also spotting what's missing on the market.

R2 - Terminology: setup and adopt a standard lexicon

- Who: EU institution
- Relevance: EU level, course providers, companies, individuals
- The adoption of a standard lexicon, including cyber role responsibilities will help companies identifying the right talent for the jobs as well as education providers to better shape their curriculum to match the cyber workforce needs.

R3 - Culture

- Who: Companies
- Relevance: companies, individuals
- People are an important asset of a company, which is reflected in its market value. There is a need to develop a cybersecurity culture on all levels of an organisation, doubled by specific tailor-made training programs to help employees and other individuals understand their roles, co-responsibilities, and facilitate accountability.

R4 - Structure

- Who: EU institutions
- Relevance: EU institutions, course providers, companies, individuals
- Use a structured approach on mapping and developing courses would be needed, by referring to a skills framework and by positioning them on the pillars of the data-driven approach.

R5 - Target

- Who: Course providers
- Relevance: companies, individuals
- Specific attention should be paid to non-ICT and non-cyber audience. Although quite a few online courses are addressing this need from a general perspective, there is little or no tailored offer for non-technical audiences impacted by cyberattacks. Examples of topics that could be addressed are Economics of Cybersecurity within an organisation, Cybersecurity for lawyers, Cybersecurity for physicians, Cybersecurity for investors.

R6 - Content

- Who: Course providers
- Relevance: companies, individuals
- Content-wise, the courses should not stay at a general level trying to address a broad cross-industry audience but should be industry-specific and built from clear learning objectives defined together with the targeted industry representatives. Irrespective of the nature of the target audience, both technical and soft (including managerial) skills should be addressed, with weights of the different subjects obviously balanced according to the specific profile of the target audience. Hands-on approaches based on real use-case scenarios tailored to the audience should be favored.

R7 - Language

- Who: Course providers
- Relevance: EU, companies, individuals
- EU is a multi-cultural continent and local language skills are important to communicate. Yet, the free movement of people comes with free movement of skills and the language should not be a barrier. Thus, in an attempt to build an international network of cybersecurity experts looking into exchanging information in support of better protecting Europe against cyberattacks, the training should at least partially be taught in English, the language of the computer (most programming languages use English language keywords). Choosing English as the main language would also increase the participation in the different MOOCs which are in their vast majority taught in English, still a barrier for non-English speakers. It will also support the mobility of cybersecurity professionals from countries with a big offer of courses, thus presumably more cybersecurity skilled people to countries with big demand in the job market.

R8 - Certification

- Who: Certification bodies
- Relevance: EU, course providers, companies, individuals
- Undoubtedly, certifications are important in the process of recruitment of cyber professionals. And at the international level, there are quite a few very specific certifications for IT professionals. In Europe though, as revealed in the ECSO study, the industry is still very dependent on US-centric certificates which are not based on formal training. And, even if in some European countries the first steps have been taken to set up a certification scheme, the uptake of these schemes is very limited. There is thus room and a need for a European Cybersecurity certification scheme for professionals. Besides, the planned European Digital Skills Certificate (EDSC) should include also cybersecurity-related skills.

R9 - European label

- Who: course providers
- Relevance: EU, companies, individuals
- European label for courses for professionals based on a minimum curriculum and including a specific percentage of topics addressing business economics and innovation.

R10 - Insurance

- Who: Insurance companies
- Relevance: companies
- Insurance companies should include in their standard portfolios, policies related to cybersecurity risks an entity could face. For example, existing offers, where available, do not cover a company's reputational damages in itself and restrict their intervention to the costs of limiting the damage to the company's reputation after an incident occurs. Since the employees are part of a firm's intangible assets, and their level of skills impacts the goodwill of the company, the inclusion of compulsory cybersecurity-related trainings offered by the company should be considered as a pro-active measure to protect the company against a cyber-attack. This measure, if properly implemented, could be enforced as a condition to the insurers to extend further their policy coverage over the company's reputational damages.

R11 - Cybersecurity Skills preparedness Radar

- Who: EU institutions
- Relevance: EU and national bodies, course providers, individuals
- A mapping of the individual EU countries preparedness in terms of cybersecurity skills would be important to be deployed. The map could display different aggregated indicators such as the country readiness to face cybersecurity challenges in terms of knowledge and skills developed via HEI and professional education, the companies HR policy linked to compulsory cybersecurity trainings, the offers of the insurance companies covering cybersecurity related risks.

R12 - Reskilling & Upskilling after COVID-19 pandemic

- Who: Member States, EU institutions, companies, schools, universities, training institutes
- Relevance: EU, member states, companies, students, workforce
- The COVID-19 pandemic emphasized one more the need for re-skilling and up-skilling for work and life, as also mentioned by JRC of the Commission with its new digital competence guidelines (July 2020) [66].

R13 - Increase Opportunities for Women in Cyber

- Who: EU institutions, Member States, companies, universities, training institutes
- Relevance: EU, Member states, companies, students, workforce
- As per the Commission's 2020 Women in Digital scoreboard, only 18% of the ICT specialists are women. Identifying and creating opportunities for Women to enter/develop a career in the Cybersecurity area. This could be implemented through different activities, between them set up an EU registry to facilitate the exchange between the already established experts while also acting as role models and possible mentors, and better balance representation of women in the cybersecurity and digital sovereignty dimensions. Good examples of initiatives that help bridge the gap are (1) the European Network for Women in Digital, (2) the No Women No Panel campaign, and (3) the Declaration of Commitment of Women in Digital.

The mapping of challenges and recommendations is depicted in Figure 6, Figure 7 and Figure 8.

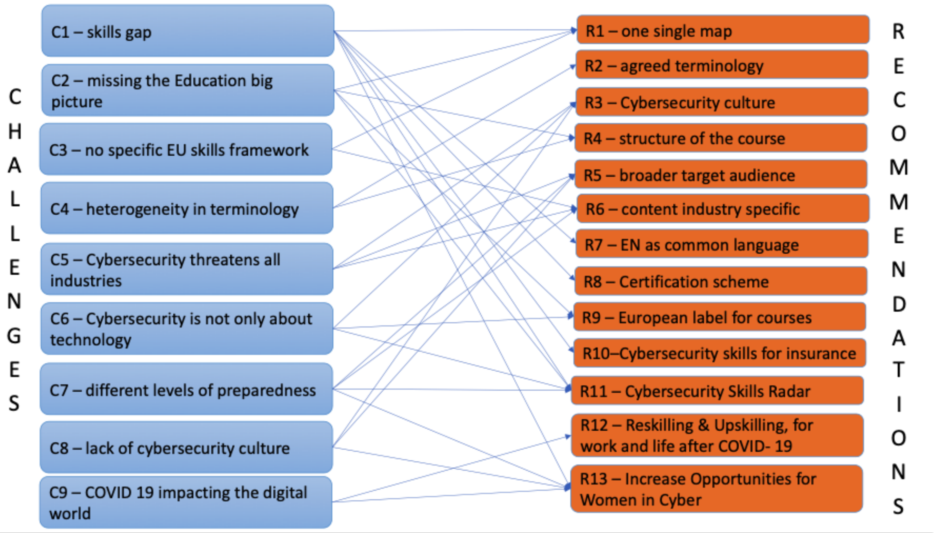
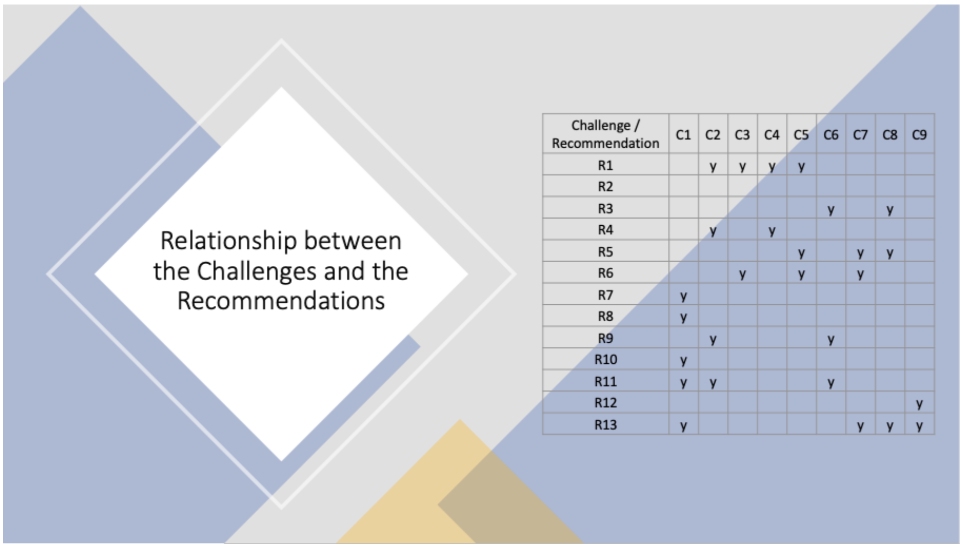

CHALLENGES
C1 – skills gap
C2 – missing the Education big picture
C3 – no specific EU skills framework
C4 – heterogeneity in terminology
C5 – Cybersecurity threatens all industries
C6 – Cybersecurity is not only about technology
C7 – different levels of preparedness
C8 – lack of cybersecurity culture
C9 – COVID 19 impacting the digital world
R1 – one single map
R2 – agreed terminology
R3 – Cybersecurity culture
R4 – structure of the course
R5 – broader target audience
R6 – content industry specific
R7 – EN as common language
R8 – Certification scheme
R9 – European label for courses
R10–Cybersecurity skills for insurance
R11 – Cybersecurity Skills Radar
R12 – Reskilling & Upskilling, for work and life after COVID- 19
R13 – Increase Opportunities for Women in Cyber
RECOMMENDATIONS

Figure 6: The relationship between the identified challenges and the proposed recommendations



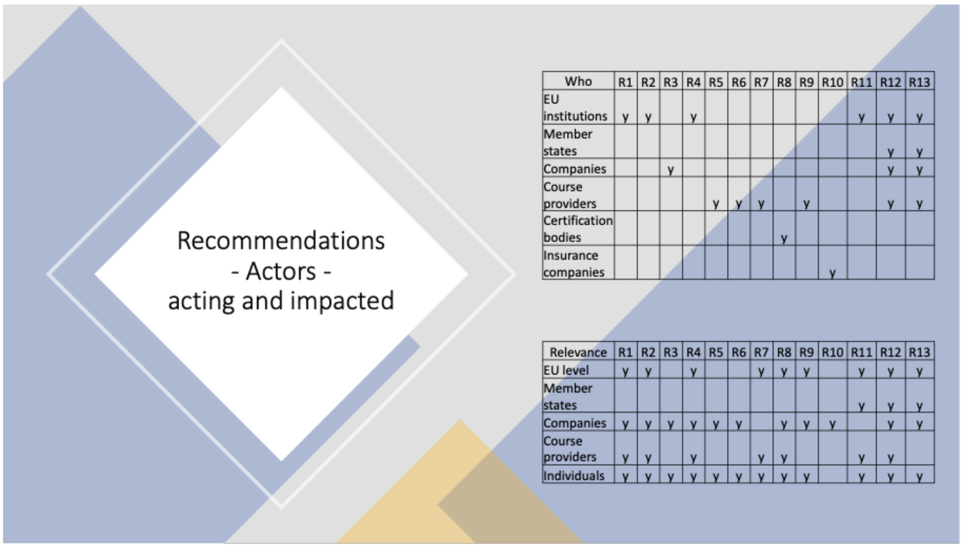
Relationship between the Challenges and the Recommendations

Challenge / Recommendation	C1	C2	C3	C4	C5	C6	C7	C8	C9
R1		y	y	y	y				
R2									
R3						y		y	
R4		y		y					
R5					y		y	y	
R6			y		y		y		
R7	y								
R8	y								
R9		y				y			
R10	y								
R11	y	y				y			
R12									y
R13	y						y	y	y

Figure 7: Mapping the Education related Recommendations to the Challenges of the sector

5.1.3 Short-Term Aims

- The design of a European Skills Framework for Cybersecurity. (R2)
- Agreeing on the common Terminology linked to Education for cybersecurity professionals (R2)


Recommendations
- Actors -
acting and impacted

Who	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13
EU institutions	y	y		y							y	y	y
Member states												y	y
Companies			y									y	y
Course providers					y	y	y		y			y	y
Certification bodies								y					
Insurance companies										y			

Relevance	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13
EU level	y	y		y			y	y	y		y	y	y
Member states											y	y	y
Companies	y	y	y	y	y	y		y	y	y		y	y
Course providers	y	y		y			y	y			y	y	
Individuals	y	y	y	y	y	y	y	y	y		y	y	y

Figure 8: Mapping of the Actors to be involved and those impacted by the proposed Recommendations

- Mapping existing courses for professionals by structuring the information based on the Skills framework and applying the Terminology (R1)
- Guidelines for course co-design and co-development with the target industry. (R6)
- The design of a Cybersecurity Skills Certification Framework that will incorporate the best practices of International Standards (R8)
- Building the Cybersecurity Skills readiness Radar (R11)
- Reskilling & Upskilling, for work and life after COVID-19 (R12)
- Increase Opportunities for Women in Cyber (R13)

5.1.4 Mid-Term Aims

- European Label for Courses for professionals (R4, R9)
- Cybersecurity Skills Certification Scheme (R8)
- Cybersecurity Skills for company insurance policy (R5, R10)

5.1.5 Long-Term Aims

- Develop the Cybersecurity culture (R3, R5)
- EN as main language for online cybersecurity courses (R7)

5.2 Education for High-School Teachers – Challenges and Recommendations

To be developed in 2021

Policy reference: Digital Education Action Plan (2021-2027)

- Strategic priority 1: Fostering the development of a high-performing digital education ecosystem

  Action: Erasmus Teacher Academies
- Strategic priority 2: Enhancing digital skills and competences for the digital transformation

  Action: Common Guidelines for teachers and educational staff to foster digital literacy and tackle disinformation through education and training

  Action: Digital Opportunity traineeships

5.3 Roadmap for Education and Skills

It is expected that certain recommendations and other details will be incorporated more extensively in the next edition of the Roadmap for Education and Skills. The visualized current version is shown in Figure 9.

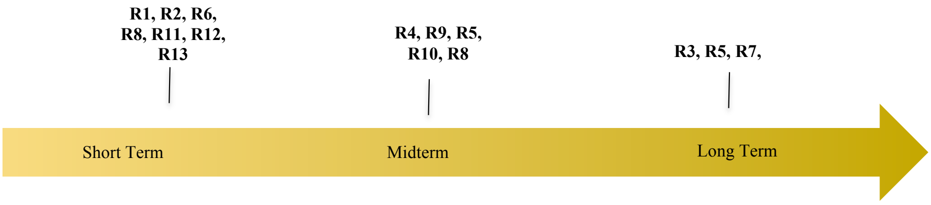


Figure 9: Overview from an Education & Skills perspective of most important directions, steps, and threats for short-, mid-, and long-term timelines linked to Professional Education

6 Roadmap for Economics

The economic dimension of cybersecurity has attracted only recent attention, although, a few steps had been performed under the umbrella of selected research projects on the national and international level during the past decade. Nevertheless, for research purposes, the design of new security algorithms, the development of quantum security, and the embedding of these and existing ones into prototypical and later vendor-specific solutions had been a major focus. Highly specialized companies develop single and multi-step technologies to counterattack a variety of security threats, as the overview of CONCORDIA's D4.1 shows. However, away from the more general approach is required to (a) understand, (b) design, (c) evaluate, and (d) apply security means for a given IT system, embedded in a larger organisation and its processes. Thus, the scope of CONCORDIA's T4.3 is especially the economic dimension of cybersecurity perspectives, which do help to determine a very useful, applicable, and concrete Cybersecurity Roadmap for Europe.

There exist only a few complementary approaches and perspectives looking at the economics of cybersecurity. Most approaches to analyse are targeting cost-benefit trade-offs faced by users, their strategic, tactical, and operational choices, and outcomes in terms of impacts for participants, which basically resembles risk assessment – frequently used for these analyses – and needs to embed this into a strong phase-based model to become applicable.

6.1 Landscape of Economics in Cybersecurity

Often systems fail because the organisations do not bear to assess the full costs of a failure neither the risks involved. This problem is prevalent in companies and end-users that present budget restrictions to invest in cybersecurity and technical expertise, such as Small- and Medium-sized Enterprises (SME) and start-ups [67]. Therefore, investments in cybersecurity solutions (e.g., based on software, services, or hardware) that not just offer protection against cyberattacks but also help during the planning and decision process of Cybersecurity is critical for the next years, which can contribute to a reduction of both CAPEX and OPEX while offering efficient protections for businesses with different demands.

Figure 10 depicts the set of key factors that have to be taken into account when considering the economic impacts of cybersecurity in business. The lack of investments by SMEs in cybersecurity, for example, is a concern for the next years. In general, these companies have restrictions and small budgets to invest in cybersecurity. Besides the fact that large companies have been investing several amounts in maintaining a dedicated cybersecurity team, the reality of SMEs is the opposite. Frequently SMEs assigned the task of protecting their systems to IT personnel who do not have adequate technical expertise in cybersecurity. Also, since they are also involved with various IT tasks, it leads to a negligence of an assessment and management of different dimensions of cybersecurity that impact the business. Concerning risk analysis and their associated economic impacts, investment

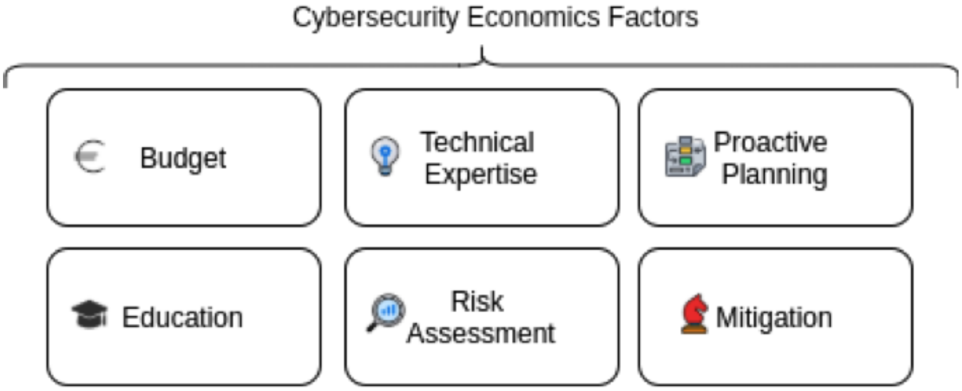


Figure 10: Key factors effecting cybersecurity economics

in education, and training activities are extremely necessary from a cybersecurity viewpoint. Therefore, it is possible to train decision-makers to analyse their systems through a holistic view, correlating the economic impacts of security activities (e.g., education, measures of prevention and remediation, insurance) with its economic impact to prevent losses from cyber insecurity. Furthermore, a well-defined and continuous education program can be taken into account to strengthen the capacity of the employees to identify and report frequent attacks (e.g., social engineering and phishing). Furthermore, education can help to build a robust Cybersecurity knowledge in the business, where can reflects on the capacity of the business to handle more complex situations such as ransomware or a botnet attack scenario.

The proactive planning for cybersecurity is also a crucial step toward a well-defined and efficient cybersecurity strategy. Thus, proactive planning should focus not only avoid attacks that can surpass the business infrastructure but also on how to mitigate or recovery from a cyberattack, such as acquiring protection services or even contracting a cyber-insurance for specific scenarios. However, before the proactive planning, it is important to conduct an in-depth risk assessment, which can identify the different vulnerabilities, attack vectors, and economic impacts of the different systems and sub-systems that compose the business. It is a critical task since a wrong assessment might result in a cascade effect, such as investments in cybersecurity and planning that do not covers the critical elements of the business.

6.2 Applied Economics Cornerstones

Cornerstones are considered to be architecturally necessary, especially to avoid the falling apart of the building. Thus, the following three dimensions determine for CONCORDIA's T4.3 these stones, which relate essential economic investigations with major security mechanisms and dedicated areas of application. Besides those three dimensions as key ones as of today, other directions might be relevant to be investigated, such as fully decentralized system architectures, Service Level Agreement (SLA) enforcement, and remote electronic voting.

6.2.1 Determination of Cybercrime Costs

Determining the costs of cybercrime is a key factor for understanding Cybersecurity from an economic perspective. However, such a determination cannot be considered to be a straightforward task, since different cost categories and elements have to be taken into account during this process. Examples of these costs include:

- Cost of anticipation, which includes preventive security means, such as access control or firewalls
- Cost of direct consequences, which includes, e.g., an interruption of service due to Denial-of-Service attacks or a reduction of availability due to unreliable communication services
- Cost of reactive security, which typically covers, e.g., restoring backups, paying fees for a certain non-compliant component, or cybersecurity insurance premiums.
- Cost of indirect consequences, which include, e.g., reputational damage, loss of confidence, or closures of the business.

A second relevant aspect is the benefit analysis in terms of a Return-On-Security-Investment (ROSI). This analysis includes links between security assurance levels and macro-economic impacts. Thirdly, the perspective to investigate societal costs, externalities, and network effects become relevant but make cybersecurity economics different. Since some economic studies of cybersecurity in the framework of demand/supply models (i.e., a cybersecurity market) exist, the decomposition into different segments (e.g., hardware, software, or services) as well as different operations and phases, become possible. Finally, further studies focus on incentives, behavioral economics (such as in the case of privacy), the economics of adversaries (attackers), cyber-insurance models, or economic effects of cybersecurity information sharing.

6.2.2 Security Analysis and Risk Analysis

One of the fundamental aspects of cybersecurity is the knowledge about the potential risk to which systems are exposed, such that a malfunctioning or a denial of services may be observed. It is important not only to determine how to analyse risks but also to determine which of these systems under analysis are critical and require adequate measures to guarantee their security at acceptable levels. Furthermore, from a generic perspective, security cannot be analysed in a fully deterministic manner, but only under certain assumptions probabilistically, i.e., there exists no perfectly secured system, which can finally resolute as secure (or even 'safe' concerning humans involved), but for an acceptable percentage of risks, thus, for a set of an acceptable level of vulnerability the willingness to accept such a system's operation, the system can be considered operational. Another factor that contributes to the increase in complexity of today's IT systems risk analysis arises from the fact that critical systems are often interconnected with other systems and faults or vulnerabilities in any of these may lead to the strong exposure of correlated others. In this context, it is imperative (a) to understand all and especially significant dependencies between complex and distributed system components (e.g., for supply-chains or eGovernment management systems) and (b) to determine, specify, and prioritize security and safety risks associated with each actor of relevance in the use case under investigation.

The essential premise to accept or refuse a certain percentage of risk invariably requires the uniform use of risk analysis approaches across multiple systems, which are based on the measurable outcome of a system's security analysis under well-defined circumstances. Systems often are vulnerable, because organisations do not take into account the complexity involved in providing a certain level of security for a large or even distributed system (i.e., correlated with other systems and subsystems as well as components). Associated costs often include two critical categories [68]:

- **Security** (prevention of malicious activities): investments are typically complex, because malicious activities typically expose externalities as a result of under-investment in cybersecurity, i.e., they usually exploit vulnerabilities unforeseen during the design space.
- **Safety** (prevention of accidents or faults): originates from requirements, which take systems failures due to unexpected events (i.e., natural disaster and/or human failures) into account to prevent the loss of lives.

A holistic and systematic view of complex systems is required to identify and isolate interfaces with directly connected systems for their assessment of risks and vulnerabilities in terms of safety and security. Besides, while the risk assessment seeks to determine exposure to vulnerabilities, the security analysis seeks to associate prevention and remediation measures in several categories, depending on the type of system in question.

For example, AFCEA (a non-profit organisation serving military, government, industry, and academia) presented a discussion on cybersecurity economics in a practical framework [69]. The framework guides private organisations and the U.S. government highlighting principles to guide investments mapping risks their associated economic impacts. Threats are categorized according to their complexity i.e., sophisticated or not, and their mission criticality i.e., define how specific vulnerability could impair a service/process.

Concerning the mapping of risks and threats, the National Institute for Standards and Technology (NIST) developed a model for guiding the investment in Cybersecurity countermeasures. Specifically, NIST's Special Publication 800-37 [70] and 800-53 [71] define the Cybersecurity Risk Management Framework (RMF) including a method for assessing the implementation of controls to mitigate risk. Although 800-37 and 800-53 do not present an analysis directly related to economic aspects, the NIST framework to classify risks, as well as the AFCEA mapping of risks, allows for the establishment of economic models based on threats. Although 800-37 and 800-53 do not present an analysis directly related to economic aspects, the NIST framework (as well as the AFCEA) to classify risks, allows for the establishment of economic models based on threats.

NIST defines risk as a function of the likelihood of a threat event happening, and the impact, the adverse effect, such an event has on the organisation [70]. Thus, measures for both impact and likelihood, and the function by which to compute the resulting risk must be defined. Given the difficulty in assigning an absolute value to these measures, it was preferred to use a five-step qualitative scale as presented in Table 4.

To estimate the risk associated with an event, first, it must be defined which the impact of this event is in case that it occurs. Table 5 presents the five steps of the impact severity.

Table 4: NIST impact definitions

Severity	**Description**
Very High	The event would have multiple severe or catastrophic adverse effects, in such a way that recovery might not possible.
High	The event would have a severe or catastrophic adverse effect, in such a way (i) to cause a severe degradation or loss in mission capability; (ii) cause major damage to assets and/or financial loss; or (iii) result in human death or injury.
Moderate	The event would have a serious adverse effect, in such a way (i) to cause degradation in mission capability but its extent and duration would still allow an organization to perform its primary functions; (ii) result in significant damage to assets and/or financial loss; or (iii) result in significant human injury
Low	The event would have a limited adverse effect, in such a way (i) to cause degradation in mission capability but its extent and duration would still allow an organization to perform its primary functions (ii) result in minor damage to assets and/or financial loss; or (iii) result in minor harm to individuals.
Very Low	The event would have negligible adverse effect.

Another valuable input for the analysis of risks is provided by ‘The Open Web Application Security Project’ (OWASP), which is an online community and non-profit organisation founded in 2001. The goal of OWASP is to produce freely available content on the topic of web application security. Since its inception it has become the de-facto standard in the field, with other reputable entities, for example, the NIST or PCI Security Standards Council regularly referencing OWASP’s work as an integral step to mitigating web application security risks. The OWASP Top

Table 5: NIST likelihood definitions

Frequency	Description
Very High	The threat source is highly motivated and sufficiently capable and is almost certain to initiate a threat event. The controls put in place are ineffective.
High	The threat source is highly motivated and sufficiently capable and is highly likely to initiate a threat event. The controls put in place are ineffective.
Moderate	The threat source is motivated and capable. The controls put in place might impede the adversary.
Low	The threat source lacks the motivation or is not capable of initiating a threat event. The controls put in place might severely impede the adversary.
Very Low	The threat source is neither motivated nor capable of initiating a threat event. The controls put in place are effective.

10 focuses on identifying the top 10 most serious web application risks in broad terms, but each organisation is unique. As such, it is important to develop a risk analysis to determine accurately the level of risk of a system.

Additionally, specific guides/frameworks exist for different cyber systems and applications. Threat modeling is a process, which identifies possible threats or vulnerabilities in the system and assesses their danger. The goal of threat modeling is the prioritization of threats, so that appropriate mitigation can be selected. For example, while NIST guides focus on the overall risks of an organisation, STRIDE [72], LINDDUN [73], or DREAD [74], map each specific type of threat as well as their mitigation actions. For instance, STRIDE (Spoofing, Tampering, Repudiation, Information (disclosure), Denial-of-Service, and Elevation of Privilege) is an industrial-level methodology that comes bundled with a catalog of security threat tree patterns that can be readily instantiated. DREAD is a mnemonic (Damage Potential, Reproducibility, Exploitability, Affected Users, Discoverability), which, although similar, represents a different approach for assessing threats. LINDDUN builds upon STRIDE to provide a comprehensive privacy threat modeling.

Aiming at the evaluation of economic risks, [75] proposes a proactive model to simulate economic risks of CNI's with integrated operations, i.e., that links many vendors, suppliers into the same ecosystem. The authors seek to map inter-dependencies amongst actors to establish a causal relation, which can be used to estimate economic risk under various scenarios. However, despite providing a view on the inter-dependencies between the actors, the proposed model does not consider problems that may later occur because of a rush to attain initial economic gains.

Cybersecurity is asymmetric by nature. For example, consider an email service in which only legitimate users can access their mailboxes: even such a system can be composed of various subsystems, such as a front-end, database, access control components, and email reading and sending components. An adversary has numerous possibilities for attacking the system. Any subcomponent could be compromised independently. An attacker for example might attack the front-end, injecting code, which when executed in the context of a legitimate user's browser, leaks information, or the attacker might exploit a vulnerability in the operating system. In contrast, engineers developing and implementing security measures must consider the security of the entire system. Covering all possible attack scenarios is simply not feasible. Thus, to discuss attack surface and attack vectors, first, it is necessary to define, which are the components to protect, and the motivation and skill level of possible attackers, to assess the probability and impact of an incident happening.

Furthermore, any rational approach in defining what is 'appropriate' involves (a) identification of risks by examining potential vulnerabilities and their chances of successful exploitation, (b) the cost of these results if vulnerabilities are exploited, and (c) the cost of mitigating vulnerabilities. The risk analysis is the fundamental stage toward mapping costs associated with Cybersecurity. It is responsible for determining, proactively or reactively, possible vulnerabilities/threats (i.e., likelihood as defined in Table 5 that may occur as a function of time as well as their associated countermeasures.

6.2.3 Structured Economic Analysis and Recommendations

The challenge concerning a structured cybersecurity economic analysis stems from the complexity to analyse the impact of successfully exploited risks in large, distributed systems since their components are often interconnected with other systems and are exposed to different types of flaws and vulnerabilities (intentional or unintended). Thus, failures or vulnerabilities in particular components of a system may lead to the failure of the entire system or directly or indirectly correlated systems, increasing the economic impact in a non-deterministic manner. For that, a framework called SEConomy [76] had been proposed to guide a structured risk analysis of a business, determined by a specific use case or IT system's installation, from a strictly economic point of view, considering that often critical and important systems or components can lead to lacking relevant investments in related security activities being neglected. These include, for example, training and education of security experts, software upgrades and maintenance, monitoring activities, among other tasks. Therefore, SEConomy describes a framework to assess the efficiency of security investments in cyber ecosystems, aiming to identify economic inefficiencies concerning the risk to which a system, its components, and related systems, which are exposed in face of its security investments.

Currently, there are many on-demand protection services and marketplaces available, which are not only offering protection services but also offer technical or organisational alternatives regarding the deployment and management of such services. However, it is not a trivial task for end-users to select any of them, since many details may not be known to the user or are omitted due to falsely assumed simplifications. For that reason MENTOR [77], a protection recommender system, had been proposed as a supporting tool for practical guidance in cybersecurity management, being able to recommend services for the prevention and mitigation of cyberattacks. The initial steps of MENTOR investigated similarity measure techniques to correlate information, such as budget constraints and the type of service required, from customers with different services available. Based on this, MENTOR can indicate an adequate service to protect infrastructures according to different demands, such as region, deployment time, and price conditions.

Although a large number of protection services are already available in the market, this number will arise together with a global deployment of novel paradigms, such as NFV and SDN. Additionally, novel business models can be used as an incentive for the development of innovative cybersecurity solutions. Based on that, a recommendation system should be able to understand the nuances of services running on different technologies to recommend a service efficiently. Besides, mechanisms to deploy the service directly on the customer's infrastructure or in a third-party host should be available, thus simplifying the process of acquisition of such protection services by non-expert end-users while reducing both Capital Expenditure (CAPEX) and Operational Expenditure (OPEX). Therefore, systems like MENTOR are important during the process of understanding and planning cost-efficient cybersecurity strategies based on the demands of a business.

6.3 Challenges

The economics of cybersecurity started more recently to become a major pillar for the operations and costs associated with cybersecurity-related investments. While the demand to provide even stronger security measures to IT system already deployed in society – starting from the individuals' home desktop, laptop, or entertainment system, reaching over to commercial IT systems of lower to higher complexity for business and production as well as maintenance use (which include society-critical processes), and leading to administrational and governmental services (including democracy foundations such as voting), is very visible in today's society, their dedicated importance does vary clearly. Due to their very high degree of interactions, embedding, and cooperation, the different stakeholders' expertise, as well as budgets, are required to be taken into consideration upon evaluating the usefulness of an IT system as a whole or a component. Only if the demanded level of 'bulletproof' characteristics can be reached for a given situation and requirements are met and provided in full, the functional operation can be assured in a more open setting of today's IT services. Thus, the cost barriers of selected stakeholder's perceptions are key and need to be identified and measured such that individual stakeholders will have the chance to determine, at which costs the demanded level of security may be reachable before the decision on certain cybersecurity mechanisms has to be taken.

Therefore, the economics of cybersecurity will pave the path for many steps to be followed soon, especially to enable an optimization of investment, installation, maintenance, and operations, and a useful update of costs. Although CONCORDIA did start this process by determining an approach for such an analysis, a much broader team of economic experts is required in very close cooperation with security experts in different industrial and governmental domains. Such collaboration can develop a more detailed, formal, and suitable model for determining impacts of implementing technological options based on a non-trustworthy and averaged or even randomized economic cost estimation, purely driven by IT departments and typically as of today still excluding proper risk assessments. One of the main challenges for a precise economic analysis of cybersecurity includes Information Asymmetry, which makes it extremely hard to determine the different information required for a precise assessment of all cybersecurity costs. This incomplete and inaccurate information results in non-efficient cybersecurity planning and investment. Therefore, main economic incentives also have to be taken into account to support suitable and privacy-preserving information-sharing regarding potential and experienced threats to create a strong, overarching community being able to share and predict major and minor economic and technical impacts of cyberattacks. Besides that, the mapping of different systems, processes, and their relations are crucial for the identification of all possible direct and indirect costs of a cyberattack.

Figure 11 provides an overview of those relevant directions, which are to be covered by academia, industry, and governments as of today. This does need a mid-term and a long-term view to reach an adequate level of Cybersecurity to reduce considerably economic impacts of cyberattacks. Different challenges will arise for Cybersecurity in the next years and decades since Cybersecurity management addresses always a moving target. As technologies are evolving fast and they become part of the entirety of today's society, such as the example with the adoption of cloud computing for many businesses and the demands on 5G as an enabler of modern mobile services, it will remain very difficult to predict impacts of cyberattacks in the future. However, it is possible to determine (a) a clear strategy, (b) a suitable model (possibly being use case-dependent), and (c) define suitable analysis frameworks and their inherent mechanisms to prepare society and businesses, who will face new threats ahead of us.

6.4 Roadmap for Economics

Based on the current set of investigations and findings of Concordia's T4.3, different aspects have to be considered to measure direct and indirect costs of the Cybersecurity and its lack thereof. For that, an understanding of legal, economic, societal, and technological aspects is essential, since every single variable can potentially result in financial losses or a business disruption. Investments in Cybersecurity are at the first glance surely not about to reach profits, but on the contrary to avoid expectable losses by knowing about threats and their countermeasures. Thus, a set of recommendations (R) is provided below, which may see changes or adaptations in how companies think about and operate with their IT investments in general or specifically. The non-exhaustive list by T4.3 includes as of below

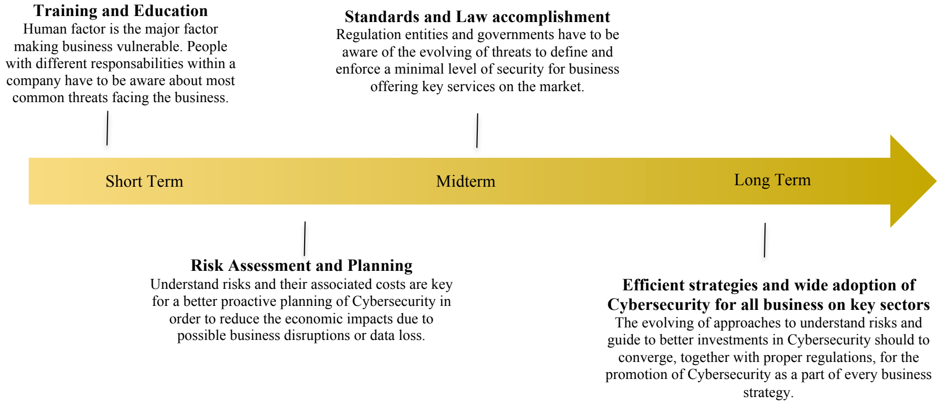

Training and Education
Human factor is the major factor making business vulnerable. People with different responsabilities within a company have to be aware about most common threats facing the business.
Standards and Law accomplishment
Regulation entities and governments have to be aware of the evolving of threats to define and enforce a minimal level of security for business offering key services on the market.
Short Term
Midterm
Long Term
Risk Assessment and Planning
Understand risks and their associated costs are key for a better proactive planning of Cybersecurity in order to reduce the economic impacts due to possible business disruptions or data loss.
Efficient strategies and wide adoption of Cybersecurity for all business on key sectors
The evolving of approaches to understand risks and guide to better investments in Cybersecurity should to converge, together with proper regulations, for the promotion of Cybersecurity as a part of every business strategy.

Figure 11: Overview from an Economic perspective of most important directions, steps, and threats for short-, mid-, and long-term timelines

relevant recommendations derived from current observations:

Based on the current set of investigations and findings of CONCORDIA's T4.3, different aspects have to be considered to measure the direct and indirect costs of cybersecurity and its lack thereof. For that, an understanding of legal, economic, societal, and technological aspects is essential since every single variable can potentially result in financial losses or business disruption. Investments in cybersecurity are at the first glance surely not about to reach profits, but on the contrary to avoid expectable losses by knowing about threats and their countermeasures. Thus, a set of recommendations (R) is provided below, which may see changes or adaptations in how companies think about and operate with their IT investments in general or specifically. The non-exhaustive list by T4.3 includes as of below relevant recommendations derived from current observations:

- **R1 - Focus on the risk assessment and planning of cybersecurity:** An essential task for any organisation wanting to gain insights into its systems' security is a risk analysis. In this task, it is essential to apply suitably (i.e., applicable for a particular system or scenario) risk analysis models to those systems in question to identify, e.g., failures and estimate probabilities of cascading failures in complex systems. Such complex systems are often characterized by the multiplicity of components or linked subsystems with which they operate in a coordinated and interconnected manner, where often failures or vulnerabilities in connected subsystems may compromise information throughout the system. In this sense, there are risk management frameworks both for mapping flaws in generic systems and specific to subsystems, which have to be observed when relevant. Once risks are assessed, the management of these risks involving possible mitigation actions involves analyzing the probabilities of such risks being mitigated. In this sense, the probability estimation is based on data available locally concerning the system's security or subsystem in question (e.g., at least for credential harvesting, mapping, and scanning behavior).

- **R2 - Efficient investments on protections:** Based on the prior understanding that recommendations are observed and applied as a whole and not isolated as such, the mapping of economic impacts (i.e., investments) occurs in mapping and risk management. In this sense, the mapping of risks and their probabilities of occurrence are a fundamental input to guide economic investments and to prioritize, in an efficient way, investments related to cybersecurity of those components and subcomponents involved. For example, it is necessary to assess trade-offs between risk probabilities and the budget available to prioritize which proactive and reactive actions can be taken. The estimated probability that vulnerabilities are exploited in non-critical systems is at certain levels acceptable to the organisation. However, the common logic of the more extensive the budget is, the more reactive and proactive risk mitigation actions are possible, results in lower risk probabilities. A typical example is related to the availability of servers in data centers, to which the less likely a server is to be unavailable, the greater the cost of the service given the different actions that a provider must take to ensure that the service will remain available. It is observed, in this sense, that actions can occur in the proactive scope as preventive measures (e.g., investment in education and up-to-date courses for professionals, monitoring and updating of components), as well as reactive measures of remediation and mitigation in case of attacks (e.g., in case of responses for DDoS attacks, exploitation of vulnerabilities, or natural disasters impacting service availability).
- **R3 - Standards and Law accomplishment:** When preparing a cybersecurity strategy, one of the critical factors is to map all required regulations correctly (e.g., GDPR) and standards to follow, while the technical functionality of the system has to remain as specified and the security dimensions to be tackled remain cost-efficient. If these requirements – typically a larger set of those, partially even contradicting – are not well-defined, many negative impacts can appear, such as penalties regarding data privacy violation, reputation harm, or even additional costs to mitigate cyberattacks, because of the absence of a clear standard to handle such situations. In the future, for example, companies that do not accomplish the EU Cybersecurity Act can see their image and competitiveness being impacted negatively.
- **R4 - Cost reduction by using state-of-the-art technologies and approaches:** Costs involved in the implementation of cybersecurity approaches are among the main factors that impact a large adoption of cybersecurity. These costs include CAPEX and OPEX. The first one is related to the acquisition of new hardware and equipment as well as new security services to handle and deal with cybersecurity, while the second one reflects the costs of operating those cybersecurity solutions. To reduce both costs and, conse-

quently, the total costs of the cybersecurity investments, trends of advanced and even new technical solutions have to be considered. For example, cloud-based solutions and NFV can play a key role in reducing CAPEX, while simplifying and reducing OPEX by sharing dedicated activities with third-party providers.

- **R5 - Training and Education:** Most of those cyberattacks known so far are dependent on a successfully performed social engineering attack, which is amplified in case of absent or very low cybersecurity education. Investment in employees' education is the key to reduce many attack vectors (e.g., phishing, ransomware, and malware). Besides that, as soon as cybersecurity becomes complex, even better training is required, which includes besides individual users CERTs, too, to react to an imminent attack efficiently. Therefore, continued training, certification, and education programs (cf. Element 4 of this roadmap) are directly related to a reduced financial loss rate due to a cyberattack.
- **R6 - Overall Integration of Cybersecurity Economics Modules within EU Cybersecurity:** As different architectures have been proposed for the EU cybersecurity, the overall integration of economics modules being offered as services part of a complete ecosystem may be beneficial for all stakeholders involved. This allows for thinking and enabling cybersecurity measurements in a technical dimension but also taking into account an integrated view combining different perspectives, such as economic, societal, and legal.

7 Roadmap for Investments

To build, achieve, and sustain European digital sovereignty we need to know where what, who, how, and when to focus on as described or otherwise identified in the other chapters of this Roadmap. We also need to know each requires substantial resources, both in people, knowledge, competencies and skills, as well in all sorts of hybrid technical and organisational infrastructures.

7.1 Multi-Dimensional, Dynamic Puzzle

Each piece of this multi-dimensional, dynamic puzzle that jointly constitutes and aims for the appropriate dynamic level of digital sovereignty requires value models, as well as business models and financial models. This, as each piece and the various dependability, interconnectivity, augmentation, and hypercubes thereof require investments, both in cash as in kind. Therewith, they also require the return of investments, being appreciated values of any kind, not only being the great value of digital sovereignty but also including (without limitation) monetary return, stakeholders value and societal value, locally, regionally, on EU level and beyond. Only investing in one or two pieces of the puzzle with not lead to a viable and sustainable ecosystem where the various returns on investments can cater to and amplify each other.

Without the appropriate returns of investments, investments of any kind are difficult to justify, and without clear purposes and arguments to invest, it will be difficult to obtain and organize the right investments from the right investors. On the latter, one for instance will need to consider the purposes and horizon of the investment necessary, the values, interests, and horizon of the various investors. Without the right balance, clear horizons, and solid footing, both short term, mid-term, and long term, we will not be able to build, achieve, and sustain European digital sovereignty.

For instance, as an example, five member states have separately commissioned to be assessed and profile from a certain perspective, called the Cyber Readiness Index [78] by Potomac Institute for Policy Studies, in which each report identifies and tries to quantify the amount a member state should invest in and what their backlog and other cybersecurity debt is – from a governmental perspective, and only to achieve certain, described goals.

For purpose of this CONCORDIA Cybersecurity Roadmap for Europe, various objectives, challenges respectively scenarios regarding or related to the most-notable investment strategies have been identified. Some of those are already highlighted below where others are merely mentioned yet under development in a stage that these are expected to be incorporated more extensively in the next edition of the Roadmap.

Obviously, among others, the Communication of the Commission (May 2020) and related updates thereto (November 2020) regarding ‘Europe’s moment: Repair and Prepare for the Next Generation’ [79], in which strategic digital capacities and capabilities are explicitly prioritised, and the (upcoming) digital investments' instruments such as Recovery and Resilience Facility, InvestEU, Strategic Investment Facility, and new Solvency Support Instrument, will be taken into account and related developments monitored, as also referred to in Chapter 1 of deliverable D4.2.

Hereunder, the currently identified objectives, challenges respectively scenarios (also collectively described as initial 'mini-roadmaps') are mentioned, each generally for local, sectoral, regional, member state, European Union team building, continuous improvement, and sustainment of European digital sovereignty and the related intertwined domains.

7.2 Objectives, Challenges & Scenarios

7.2.1 Objective: Landscaping H2020 Cybersecurity Deliverables

State of Play (SOP): Currently and in the past period the Horizon 2020 funds have been allocated to quite some extent to projects focussing on or otherwise addressing cybersecurity and related topics regarding or related to digital sovereignty. However, there is no clarity, overview, or useful insight available whether and to what extent project results are concrete, viable, effective, and sustainable to add to the building, achieving, and sustain European digital sovereignty.

State of the Art (SOTA): Having a clear, practical, and otherwise useful landscape of the H2020 cybersecurity deliverables and other results is recommended. It can give oversight and insight into what has already been done, where it can be deployed and further developed, and what is still missing. Just mapping those geographically is not enough; the various deliverables and results – and where available post-project dissemination activities – will need to be vetted at merit. The other main objective is to identify synergies, gaps, and improvements, and use these for consideration for (further) investments and the like. Where possible, one can also consider inviting, assess, and where appropriate add the deliverables and other results from similar cybersecurity-related projects of member states or regions as well. This, also to involve member states and regions in this effort.

GAP (SOTA -/- SOP): The initial main GAP is the lack of mapping about the identified H2020 cybersecurity deliverables and other results to the extent deemed sufficiently concrete, viable, effective, and sustainable to add to the building, achieving, and sustain European digital sovereignty, starting with structured visualisation in identified cybersecurity domains and dimensions of (to be assessed and otherwise collaboratively and multi-angled vetted) cybersecurity research activities, innovation activities, and related products, systems, services or other capabilities of European organisations that are active in the cybersecurity domain. Thereafter, synergies, gaps, and improvements can be identified, and used for various purposes, including for consideration for (further) investments and the like, to facilitate the building, achieving, and sustain European digital sovereignty. For such vetting purposes, for instance, the various angles of the evaluation components and queries of the European Innovation Council (EIC) and related lessons learned could be considered and optimised to the purpose and particulars of the mapping and plotting described above.

Short-Term: For the Short Term, bridging the initial main GAP a cross-EU initiative is necessary by mapping and plotting the landscape of H2020 (and related) cybersecurity deliverables and other results on the one hand and the various identified market needs, cybersecurity and vulnerability developments and predictions on the other hand. Where relevant, these could be, amongst others, linked with the Open Research Europe initiative that has just been launched by the Commission, the Cybersecurity Atlas, and the like.

Mid-Term: For the Mid-Term, building on the results – including the mapping and plotting as set forth above – from the Short-Term activities: knowing what viable deliverables and other results are already readily available, knowing how and with whom to (help to) operationalise, deploy and sustain those, including knowing where and how to join forces, invest in and what the sought-after various values and returns of investments are, are prerequisites for European digital sovereignty.

Long-Term: Where not yet achieved in the Mid-Term, such oversight, insights, and deployment as set forth above should be further pursued. In any case, these should be the basis for a supplement, keeping up to date, evaluating progress – also regarding investments and returns on investments –, improvement and otherwise optimisation.

Conclusions: Where the EU has already funded numerous projects in the various Framework Programs including Horizon 2020, and it will continue to do so in subsequent programs such as Digital Europe and Horizon Europe, amongst others, this gives an excellent opportunity to build up, double-loop and further improve capabilities necessary for European digital sovereignty.

7.2.2 Challenge: Narrowing the Investment Gap

State of Play (SOP): Where early-stage cybersecurity companies and other ventures are being heavily funded in other parts of the world, such business angle and other venture capital by Europeans or European organisations, as well as subsequent financing by European organisations, either public, private or other sectors, still is at a relatively yet dangerously low level within the European Union. In short, the European Union, its member states, and related sectors and organisations are outspent and outsmarted substantially. European grass-rooted initiatives, ventures or businesses, whether early-stage, SMEs, intrapreneur or otherwise, stand no chance to remain truly European if they would have the ambition to become a significant market player of any kind, and are acquired or otherwise not European anymore before they can seriously growth, scale and become European champions in their respective markets. This clearly undermines European digital sovereignty.

State of the Art (SOTA): The envisioned state of the art is obvious; building European organisations with cybersecurity capabilities that the European sectors and markets – as well as markets outside of the EU – want and pay for while staying, and that can grow, scale and succeed while remaining truly European. One of the main components is to narrow the investment gap.

GAP (SOTA -/- SOP): The initial main GAP is the lack of mapping about the currently fragmented and seemingly not orchestrated public and private investments in the EU and its member states, including the various stakeholders in this landscape, either being truly European or otherwise. Teaming up from the European perspective for digital sovereignty starts with transparency of and appreciation by the relevant stakeholders – which are not merely financial investors, whether public or private –, and their respective and various values, perspectives, needs, and interests. Such insight and oversight lead to trust, necessary to identify and discuss if, what, and to which extent European synergies, investments, and returns on investment could and should be considered, and furthered towards deployment, nurturing, and monitoring. There need to be sufficient levels of transparency, trust, willingness, comfort, and execution power. To be clear, not only a substantial amount of structural and ongoing financial investments needs to be enabled and facilitated. The qualitative objectives, values, coordination, governance, returns, and other interests need to be very clear on a detailed level and need to be continuously optimized as per the dynamics in this Digital Age. Merely making available monetary sums will not lead to success towards European digital sovereignty. Next to solid financial investment, vital non-financial and other qualitative attention is necessary. Obviously, it is recommended that the GAP can be taken one step or one domain or risk-dimension at a time, to try, learn, pivot, and improve. Meanwhile, it is relatively easy to discuss, architect, and prepare various relevant scenarios of potential events or occurrences that may arise or happen in the domain of European digital sovereignty.

Timeline: Various multi-speed tracks can be identified and run parallel. Otherwise, the Short Term is recommended to kickstart, discuss value propositions and expectations of various returns of investments, while starting with architecting scenarios, and both Mid Term and Long Term to prepare, organise, execute, monitor, improve and sustain are essential. Narrowing the investment gap will be a dynamic and ongoing topic, that will need constant attention and agility.

- **Short-Term:** For the Short-Term, bridging the initial main GAP cross-EU initiative is necessary to map and plot the various landscapes and meta-landscape and its respective stakeholders, identify and discuss value propositions, business models, financial models, and expectations of various returns of investments. Meanwhile, starting with architecting relevant scenarios will help to identify the various benefits and preconditions and establish which appropriate net benefits are envisioned.

  Mid-Term: For the Mid-Term, insight and oversight will grow to a level scenarios can be operationalised, and deployed. Starting relatively modest yet in a way that can scale and agility to evolve and be improved is recommended. As appreciation within the EU is sought after, some traction and growth of the willingness to invest and alignment to investments are expected to increase. Further organising, executing, monitoring, and improving is essential. Depending on the uptake, narrowing the investment gap can hopefully already be scaled in the Mid-Term.

  Long-Term: Where not yet achieved in the Mid-Term, narrowing the investment gap can be scaled in the Long Term. As mentioned, narrowing the investment gap will be a dynamic and ongoing topic that will need constant attention and agility.

Conclusions: There are various paths to address the challenge of narrowing the investment gap. Considering, operationalising, and incentivising investments require knowing the various needs, stakeholders, values, interests, and horizons as well. Addressing all relevant sectors in the whole single market to build, achieve, and sustain digital sovereignty will be too ambitious, but starting anywhere in a diligent, scenario-based way as soon as possible is highly recommended.

7.2.3 Other Objectives, Challenges or Scenarios

Other objectives, challenges, or scenarios regarding investment strategies are under investigation and development as a mini-roadmap, and are currently anticipated to reach a certain level of maturity and detail to be included in subsequent Roadmap edition(s), including the following:

- Objective: European Fund for Digital Sovereignty Capabilities & Continuity. This mini-roadmap is envisioned to enable the European Union, member states, and other stakeholders to leverage their combined investment capacities, align and federate existing and envisioned hybrid investment instruments and create a European Fund for Digital Sovereignty Capabilities & Continuity, and;

- Some objectives, challenges, or scenarios that are defined elsewhere in this Roadmap, but then where relevant developed from the investment strategies angle.

7.3 Roadmap for Investment Strategies

It is expected that certain recommendations and other details will be incorporated more extensively in the next edition of this roadmap. The visualized current version is shown in Figure 12.

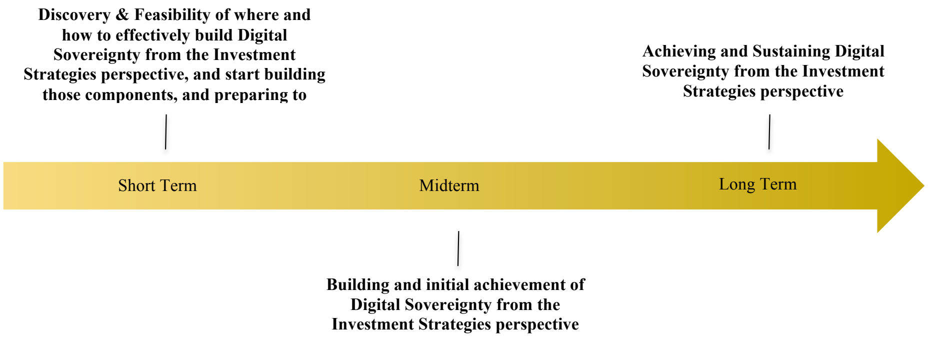

Discovery & Feasibility of where and how to effectively build Digital Sovereignty from the Investment Strategies perspective, and start building those components, and preparing to
Achieving and Sustaining Digital Sovereignty from the Investment Strategies perspective
Short Term
Midterm
Long Term
Building and initial achievement of Digital Sovereignty from the Investment Strategies perspective

Figure 12: Overview from an Investment perspective of most important directions, steps, and threats for short-, mid-, and long-term timelines

8 Roadmap for Legal and Policy

For organisations in any and every sector in member states, the EU and around the world, implementing state-of-the-art security, privacy, cyber-physical safety, (personal and non-personal)) data protection, cyber resilience, transparency, and accountability (using both technical and organisational measures) are now a must in this Digital Age. The level of dependability and the level of ever-increasing dynamics justify that and is proven daily. It is challenging our Digital Sovereignty and our Rule of Law, both on the European level and member state level.

This leads to many and various challenges to address, risks to mitigate, impact to avoid, re-organise or otherwise coordinate and orchestrate detrimental consequences and related responsibility, accountability, liability, and enforcement capabilities, as well as renewed or otherwise improved monitoring and supervising in this Digital Age. While the existing policy instruments of all sorts, the efficiency of governmental authorities, as well as existing legal structures, responsibilities, measures, remedies, and other capabilities are challenged, these are – in an improved, transparent and accountable way – for sure also part of the solution.

8.1 Build, Achieve & Sustain Digital Sovereignty

However, it also leads to many and various opportunities to identify, grasp, embrace, incentivise, and otherwise organise, endorse, and augment. Policy instruments of all sorts, and related improvement of transparency, implementation, interpretation, living lab capabilities, inclusion, maturity and consistency of authorities and law enforcement, cross-sectoral and cross-member state public-private cooperation, co-creation, common understanding, joining forces and related trust and trustworthiness are very powerful – and prerequisite – tools and means to build, achieve and sustain Europe fit for the Digital Age including future-proof Digital Sovereignty.

Meanwhile, we have to accept – and embrace – constant change. The vast domain of cybersecurity amplifies this notion on a 24/7 basis. Developments such as 5G further amply these with a factor of 100 or more. This also leads to the need to rethink f what and how policy instruments can be deployed and kept up to date with the ever-evolving and increasing dynamics of this Digital Age. Static (policy) instruments in a dynamic digital and cyber-physical world will generally not anymore be up for the job they were intended and designed for.

Said differently, in this Digital Age, digital technology and cyber-physical ecosystems have outstripped our societal, economical, and legal frameworks. How to catch up? And, how to keep up?

For that, aiming to and supporting jointly creating, building, achieving, and sustaining European digital sovereignty (including the related intertwined symbiosis of collaborative resilience, research and innovation, education, skills and jobs, and economic development and competition) is definitely an excellent main mis-

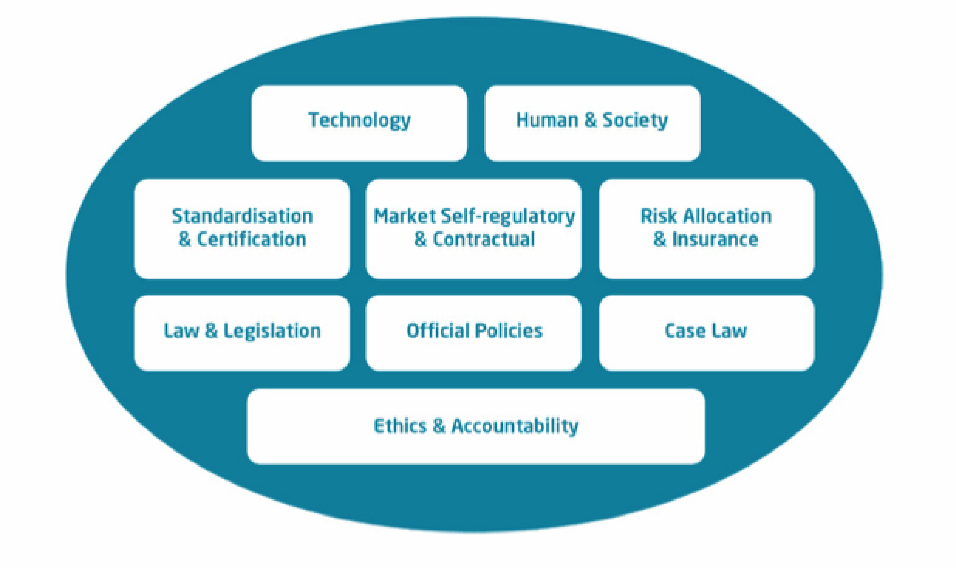

Technology
Human & Society
Standardisation & Certification
Market Self-regulatory & Contractual
Risk Allocation & Insurance
Law & Legislation
Official Policies
Case Law
Ethics & Accountability

Figure 13: Ecosystem for technology & the Rule of law

sion to focus on. 21st century and future-proof legal and policy strategies are one the essential core components to make it work.

For purpose of this CONCORDIA Cybersecurity Roadmap for Europe, various objectives, challenges respectively scenarios regarding or related to most-notable legal and policy strategies have been identified. Some of those are already highlighted below where others are merely mentioned yet under development in a stage that these are expected to be incorporated more extensively in the next edition of the Roadmap.

For the avoidance of doubt, obviously numerous open source publications have been read and assessed (next to others for instance mentioned in D4.2), such as for example and in random order: (i) EPRS Ideas Paper Towards a more resilient EU, about Digital sovereignty for Europe [2], (ii) Report from the EU Court of Auditors [80] stressing that more EU action is needed to address inconsistent transposition or gaps in EU law (e.g. limited and diverse legal frameworks for duties of care; the EU's company law directives have no specific requirements on the disclosure of cyber risks), (iii) Consultation Paper by ENISA about EU ICT Industrial policy in cybersecurity context [4], (iv) Cyber Readiness Index Country Profiles [78] of the five member states that have been reported by Potomac Institute for Policy Studies, (v) the National Cyber Security Strategy paper by ENISA[81], and (vi) the draft Union Rolling Work Program for European cybersecurity certification, amongst many others.

8.2 Objectives, Challenges & Scenarios

Hereunder, the currently identified objectives, challenges respectively scenarios (also collectively described as initial ”mini-roadmaps”) are mentioned, each generally for local, sectoral, regional, member state, European Union team building, continuous improvement, and sustainment of European digital sovereignty and the related intertwined domains.

8.2.1 Objective: Trusted Experience Sharing

State of Play (SOP): Within the EU and the member states and their respective regions and local public and private organisations in every sector, there is a wealth of knowledge, experience, lessons learned, and best practices (collectively: ‘Experience’) available in the EU, its member states and its organisations and individuals.

Each has a particular Experience, but as per the dynamics of digital ecosystems, actors and the (mis)use it is not sufficient or otherwise run obsolete quickly, although each does not necessarily need the same amount of Experience as everybody else. This, as each context, is different and requires other Experience. Furthermore, some are more experienced, mature, or active in certain domains where others are not.

Currently, there is no trusted Experience sharing ecosystem of ecosystems where omni-stakeholders can share, exchange, and otherwise take in the Experience of others. Most Experience therefore is not shared and not re-used. This wealth of Experience generally goes to waste.

State of Art (SOTA): Trusted Experience sharing starts with transparency of stakeholders, and their various values, perspectives, and interests. Such insight and oversight in transparency and appreciation lead to trust. Consistency thereof will build and cater more trust down the road.

Said otherwise, one of the main core components would be to have a clear stakeholders landscape, and based on that the stakeholders getting and learning to know, understand and appreciate each other, also cross-sectorial, cross-regional, and across networks. A next step thereafter enabled and facilitated will be the sharing trustworthy Experience in a trusted way: Trusted Experience Sharing.

GAP (SOTA -/- SOP): The initial main GAP is the lack of mapping about the various stakeholders in this landscape. Trusted Experience sharing starts with transparency of and appreciation by stakeholders, and their respective and various values, perspectives, needs, and interests. Such insight and oversight lead to trust, necessary to discuss the multi-layered architectures that enable and facilitate trusted Experience sharing. There needs to be a sufficient amount of trust before one will share. Thereafter, the sharing itself needs to be done in a trustworthy and consistent way as well.

With that one can take stock from member states level Experience regarding Digital Sovereignty & Collaborative Resilience, and also become future-proof and otherwise resilient on EU level, as well as vice versa: how to take stock from EU level Experience and become future-proof and otherwise resilient on a member state level. This wealth is to be organised, nurtured, structured, systemized, and built on for European digital sovereignty.

Timeline: Short-Term to kickstart and assess, and both Mid Term and Long Term to scale, improve, and sustain are essential.

- **Short-Term:** For the Short-Term: for bridging the initial main GAP a member-state and cross-EU initiative is necessary to map and plot the landscape and its stakeholders.

  This is different than the current Cybersecurity Atlas initiatives. The Cybersecurity Atlas helps on certain identification and mapping on organisation level and as per the current purposes of the Atlas mostly on research. The mapping and plotting with the purpose for Trusted Experience Sharing is as outlined in the paragraph GAP, above, including available, requested, required, and missing capabilities and competencies, including its needs and other related Expertise. Such should also not be in the public domain per se, such as the open-source parts of the Cybersecurity Atlas. The envisioned outcome of the short-term activities would be transparency of and appreciation by stakeholders, and their respective and various values, perspectives, needs, and interests.
- **Mid-Term:** For the Mid Term, insight and oversight will grow to a level where multi-layered Experience sharing architectures can be discussed and designed that enable and facilitate trusted Experience sharing. Starting relatively modest yet in a way that can scale and agility to evolve and be improved is recommended. Depending on the uptake, the Experience sharing network can hopefully be scaled in the Mid-Term.
- **Long-Term:** Where not yet achieved in the Mid-Term, the Experience sharing network can be scaled in the Long-Term. In any case, resilience, sustainability, and continuous enrichment, and other improvement should be part of the Long-Term efforts.

Conclusions: Knowing what we already have, knowing where one can help and otherwise support the other, and knowing who to join forces with where white spots of Experience need to be addressed is a prerequisite for European digital sovereignty. Without knowing, in cybersecurity and another sovereignty context a malicious actor will find the weakest link or other weak access points for exploitation and the like. Regarding the latter, we all should be aware that those actors to collaborate with each other. It is up to us to do the same.

8.2.2 Objective: EU Landscaping of Products, Systems & Services

State of Play (SOP): Cybersecurity is a very important and seen from all angles interesting domain; even the smallest connected device nowadays can add to major disruptions. As cybersecurity is a horizontal and cross-cutting topic, and as it is relevant in any and all layers of both the technical systems as well as organisational and societal ecosystems, there is no person or organisation – whether in the public or private sector – for which cybersecurity is not relevant and does not have a potential negative impact.

However, the cybersecurity domain is vast, fragmented, and not well-defined. At the same time, attack strategies are constantly shifting, and the impact is becoming exceedingly high. While the urgency to understand and deal with these new attacks is increasing, there are not enough companies and other organisations that can formulate concrete responses to these new threats. To add to that, as digital and related technology in the connected, hyper-connected, converging world (physical, cyber, and cyber-physical) changes the world at such a fast pace, and is relatively new for organisations – whether on the supply side or on the demand or end-user side –, the maturity level of society is below par.

Most of the member states have identified cybersecurity as not only an important and prerequisite domain and topic to address continuously, but also as an enabler and opportunity to build on, excel, and become digital sovereign as a member state and European Union Digital Single Market.

However, it is not easy to landscape the vast and dynamic cybersecurity domain. Even ENISA, NIST as well as Gartner, and other organisations do not identify, landscape, and map all parts of this domain. Nor do they make their frameworks non-academic, i.e., readable for a wider audience. Furthermore, it is not easy to understand the various and generally not very transparent propositions of cybersecurity organisations and the products, services, and systems they factually develop and factually market. With that, it is also very hard to analyse these in-depth in such a way that is recognizable, practical, and useful to work with. Yet one can map out and execute strategies and tactics to take stock and convert this knowledge and experience into opportunities and enablers for companies, organisations, economy and to benefit European Union society, including without limitation economy, as a whole.

State of the Art (SOTA): Adequate and comprehensive cybersecurity frameworks, also acknowledging that the cybersecurity domain continuously expands. Next to that, it is hard to spot and select the right players in the market, which makes diligent and effective matchmaking a tedious task.

With this, both demand side, vendor side, researchers and (other) academia as well as the public sector, member states, and the Commission and related agencies would know what European Union cybersecurity organisations actually and factually have to offer, what not, who could or should team up with whom, and where the gaps are that needs consideration, action or other (urgent or other) intervention. In this way, relevant stakeholders could and should be connected even more to prepare and continuously build resilience against both the threats of today and those in the future.

GAP (SOTA -/- SOP): The initial main GAP is the lack of mapping about the actual, vetted cybersecurity capabilities and offerings of European organisations, starting with structured visualisation in identified cybersecurity domains and dimensions of (to be assessed and otherwise collaboratively and multi-angled vetted) cybersecurity products, systems and services of European cybersecurity companies that are active in the Cybersecurity Domain.

Thereafter, certain analysis of the gaps between the identified cybersecurity domains and dimensions on the one hand and the various identified marketed cybersecurity products, systems, and services, on the other hand, will give oversight and insight in the gaps from angles such as without limitation risk, impact, geolocation, industry/market segment, compliance, best practices, standards, regulation, collaboration, market optimisation, market opportunities, research opportunities, competition, and other digital sovereignty relevance. This enables and facilitates the SOTA, while being the basis for the supplement, keeping up to date, improvement and otherwise optimisation possible.

Timeline: Short-Term to kickstart and assess, and both Mid-Term and Long-Term to scale, improve, and sustain are essential.

- **Short-Term:** For the Short-Term, bridging the initial main GAP a member-state and cross-EU initiative is necessary by mapping and plotting the landscape of cybersecurity domains and dimensions on the one hand and the various identified marketed cybersecurity products, systems, and services on the other hand.
- **Mid-Term:** For the Mid-Term, building on the results – including the mapping and plotting as set forth above – from the Short-Term activities: knowing what we already have, knowing where one can help and otherwise support the other, and knowing how to join forces where white spots of Experience need to be addressed is a prerequisite for European digital sovereignty.
- **Long-Term:** Where not yet achieved in the Mid-Term, such oversight, and insights as set forth above should be further pursued. In any case, these should be the basis for sustainment, supplement, keeping up to date, improvement, and otherwise optimization.

Conclusions: Knowledge provides insights and oversight. Without knowing, also in cybersecurity and another sovereignty context, no appropriate and contextual team building will be possible to help identify, assess, make aware, protect, detect, alert, respond, recover, report, and continuously improve products, systems, and services used, deployed, implemented, developed, pre-procured or procured. This would lead to a lower level of or no European digital sovereignty, which is obviously not recommended.

8.2.3 Objective: Member State NIS Directive Comfort & Capability Building

State of Play (SOP): The current NIS Directive, which is under review, generally aims to enhance the readiness in particular sectors responsible for critical infrastructure, vital systems respectively essential services as defined therein. Compared to other critical infrastructure regulations outside the EU, the NIS Directive is state of the art. However, not all sectors mentioned in the NIS Director are covered by each member state. Even more, there is quite some difference in the sector-coverage by each member state under the NIS Directive. Some member states have up to four (4) times more sector-coverage than the other. In short, the levels of implementation differ substantially.

This at least reduces the operational effectiveness of responses to large-scale cybersecurity incidents or zero-day vulnerabilities. It also reduces the effectiveness of the strategy of the NIS Directive, and any success to build, achieve, and sustain digital sovereignty within the European Union.

State of the Art (SOTA): Vulnerabilities in critical infrastructure, vital systems, and essential services do not stop at any member state border (let alone the EU outer-borders). A particular challenge for the Commission and member states is encouraging other member states to adopt and implement the same level of sector-coverage as the other member states, or at least to a certain minimum yet sufficient level.

GAP (SOTA -/- SOP): Identifying and addressing each reason for the difference in levels of implementation is the only way to support building, achieving, and sustaining digital sovereignty of European (member state and related) critical infrastructure vital systems and essential services. This, as the weakest link, can expect to be the main attack vector. But, also, as the systems are generally interdependent, influence each other, and can infect or negatively affect each other. Reasons could be the lack of expertise to implement in a particular sector, potential hurdles or other preconditions, or the lack of resources, funds, or other capabilities.

Addressing these in a relatively modest way is recommendable. For instance, on a sector-by-sector basis, where the sector is addressed that adds the most appreciation to the respective member state where it may also be the one that brings synergies to the resilience of interlinked sectors in such member state or even augment resilience to the similar sector in other member states.

Timeline: Short-Term to kickstart and assess, and both Mid-Term and Long-Term to scale, improve, and sustain are essential.

- **Short-Term:** For the Short-Term, identifying and addressing each reason for the difference in levels of implementation is recommended, including finding the true reasons and possible solutions to address those (including within limitation any precondition or impact such solution may have respectively created itself) and facilitating understanding and appreciation.
- **Mid-Term:** For the Mid-Term, support implementation in a non-intrusive and respectful way, where it is recommendable to initially have a relatively modest implementation speed, and only speed up where it may be possible and comfortable for the respective member state, sector, and related stakeholders. Meanwhile, it is also recommended to identify and visualise the output, synergies, and other results – including lessons learned –, also for

potential (re)use in other NIS sector implementation, either in the respective or other member states.

- **Long-Term:** For the Long-Term, the sector-by-sector implementations can be completed to the extent agreed and continuously improved as the cat- and mouse game with the malicious actors will be continuous as well.

Conclusions: Supporting member states and related NIS sectors with the appropriate level of comfort and sufficient and adequate capability building is seen as a major contribution to digital sovereignty, both for member states, sectors – both public and private – as well as the European Union, and its periphery.

8.2.4 Challenge: How to Operationalise Europe's Championing of Human-Centric Values

State of Play (SOP): In this Digital Age, and also because of that an increasingly globalised world, the European Union is generally seen as a leader regarding human-centric values such as those reflected and implemented in the GDPR. The GDPR is already either copied or inspired by many countries around the world.

However, the GDPR is the successor of the 1995/46 EC Privacy Directive, so this human-centric regulation is already 25 years old and was implemented before the internet went from nice-to-have to a need-to-have and from an international network used by academia to a global network used by everybody. It is one of the indicators that the EU's normative power alone cannot guarantee the European digital sovereignty of its citizens, businesses, organisations, society, and economy. Neither can it guarantee that human-centric policy instruments give the European Union, its member states, citizens, and organisation a competitive edge both in the EU as well as when exporting abroad.

State of the Art (SOTA): Leveraging the human-centric values approach to a level that can be operationalised, monitored and enforced – also by citizens and organisations themselves within the Rule of Law –, in a European Union-wide clear and transparent way. This, also to export these frameworks, good practices and lessons learned beyond the European Union, and to have the ability to market these value-centric digital products, systems, and services abroad. It strengthens both the digital sovereignty of within the EU as well as – at least on conceptual and principle-based level – of and within other countries and regions in the world. Furthermore, it can bring benefits to the European private sector, both vendor side as demand side, as more GDPR-proof or other human-centric digital products, systems and services can be exported or otherwise offered to (respectively can be procured from) a global market with the same of similar digital sovereignty objectives.

GAP (SOTA -/- SOP): There are basically two main bridges possible to get to the SOTA, as each will take different efforts and have different timelines. One is to initially identify, mapping and plotting the member states, regions respectively states that have, in either substantial or certain parts, found inspiration from the

GDPR and have or are working on implementing it locally, regionally, or nationally. This, to reach out, link up, and learn from choices make, lessons learned, improvements planned, and monitoring or enforcement made more efficient and transparent. The GDPR obviously is just one example of human-centricity, but currently the most mature to focus on.

The other main bridge could be to use the first bridge outcomes to discuss, identity and where feasible deploy and monitor improvements to means, measures, and other policy instruments (without revising the GDPR in any way) in order to enable European citizens, data protection authorities and other stakeholders to more effectively enforce their respective rights or help enforce the respective rights that are so essential for digital sovereignty. Digital sovereignty starts with sovereign citizens, communities, and local society.

Timeline: Short-Term to kickstart and assess, and both Mid-Term and Long-Term to build appreciation and operational collaborations, develop future-proof measures, for deployment in living labs first with the ability to scale, and later on the scale, improve and sustain those are essential.

Conclusions: The European Union, its member states, citizens, and organisation have something very valuable – and sought after globally – to offer: implemented human-centric value policy instruments such as the GDPR. It can both bring wealth and digital sovereignty to our allies and friends outside of the EU, as it can bring prosperity and digital sovereignty to EU's and member states' citizens, communities, society, and economy.

8.2.5 Objective: EU Pre-procurement of EU Products, Systems and Services

State of Play (SOP): Whether one likes it or not, technology changes the world at a fast pace, so better embrace it. Digital ecosystems, cloud computing, edge, Internet of things, spectrum, cybersecurity, data management, and the like are what organisations are talking about daily and are increasingly assessing the opportunities, benefits, and risks. Technology makes innovation possible, and technology is a need-to-have in organisations, society, and the economy. It is essential for the successful and future-proof operation of an organisation. It can be the difference between an incumbent with no future continuity and no relevance, and one that is ready for the future.

However, most organisations do not know what they need, what to procure, and how to procure including all relevant elements, components, functionals, and non-functionals – including without limitation cybersecurity – to create its own digital sovereignty, and with that add and augment the digital sovereignty of its sector, market, member state, and the digital sovereignty of the European Union.

State of the Art (SOTA): There is no joint-procurement framework for cybersecurity infrastructure, let alone a dynamic pre-procurement model with which one can make its own informed decision. The same goes for the essential and various combinations of digital functionals, non-functionals, and capabilities that make a digital ecosystem, platform, product, or service.

Without such dynamic pre-procurement and procurement comfort and capabilities, there will be no successful engagement possible between organisations, vendors, staff, customers, and society. At the same time, given the increasing dependability on and complexity of digital technology and digital ecosystems, organisations generally do not know what they need, what to procure (pre-procurement), how to procure it, how to negotiate out such technology arrangements (either platforms, digital ecosystems, networks, technology-as-a-service (xaaS) or otherwise) and how to keep it optimized and to monitor it continuously.

GAP (SOTA -/- SOP): Applying easy to implement good practices such as a three-phases methodology visualised below, and using proven common reference models about performance, cybersecurity, data protection and data management, and negotiation capabilities to pre-procure and procure 21st-century technology including the appropriate levels of trust, security, safety, protection and management capabilities can help to navigate organisations during their effort to both stays or become more resilient and competitive as well as support the digital sovereignty of such organisation as well as its network, sector, member state, and the European Union. It enables and facilitates making informed decisions and a decision model that helps to ensure compliance with regulatory frameworks and industry standards, and, thus, facilitates increasing trust and trustworthiness.

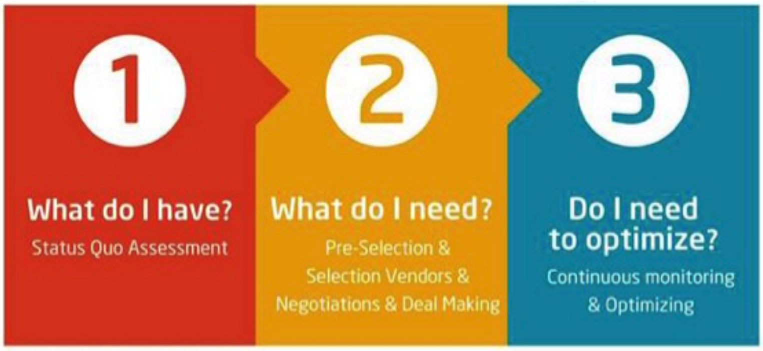


Figure 14: Three Phase Methodology

Timeline: Short-Term to kickstart and assess, and both Mid-Term and Long-Term to scale, improve, and sustain are essential. A well-defined strategy concerning pre-procurement, procurement, and continuous monitoring and optimisation for the short, mid-, and long term is recommended.

- **Short-Term:** For the Short-Term, the various methodologies and other best practices should be identified, vetted, tested, and further improved, whereafter a controlled, relatively modest deployment is recommended to commence, for instance in a certain sector or a certain group of organisations.
- **Mid-Term:** For the Mid-Term, focussing on certain sectors or groups of organisations is recommended to help increase both the appreciation of these

pre-procurement capabilities as well their competitiveness on the market, including mitigating becoming an irrelevant market player, and their ability to offer European, superior, state-of-the-art products, systems and services and the resulting increased consumer and other market trusts.

- **Long-Term:** For the Long-Term, the more challenging sectors, or groups of organisations can be enabled and facilitated to deploy these pre-procurement capabilities, including structured, modular architectures, data-centric, technology- & vendor-neutral and by-design approach following the most demanding regulatory frameworks and industry standards.

Conclusions: The objective is to support European organisations, whether public or private sector, and whether small, SMEs, midsized or large, to make informed decisions and give them future-proof capabilities to prepare, create transparency and trust and build agility and resilience for the Digital Age and new markets, transformation, convergence, and competition. Hence, an organisation will be able to remain relevant with the potential of becoming a market leader in fields that shape the future, and the future of your organisation, both in the European Union as well as globally.

8.2.6 Other Objectives, Challenges or Scenarios

Other objectives, challenges, or scenarios that are under investigation and development as a mini-roadmap, and that are anticipated to reach a certain level of maturity and detail to be included in subsequent Roadmap edition(s) currently are:

- **Objective: Trust & Trustworthiness By Design for Cross-Sectorial Convergence.** This mini-roadmap is envisioned to focus on digital ecosystems in multiple sectors, and how to go from a trusted and trustworthy single component to a trusted and trustworthy end-to-end system, where multi-use (other than a single intended use approach) – including unintended use – is the default.
- **Objective: Data-Supported, (Near)Real-Time Transparency & Accountability.** This mini-roadmap is envisioned to focus on both (A) digital sovereign authorities, that are well-equipped for the Digital Age (including without limitation with transparent and trustworthy digital means), well-sourced, well-endorsed and can operate independent yet accountable (also while addressing the vault-lines between privacy and freedom on the one hand and surveillance and national security on the other) in accordance with their mandate, and (B) means that support with data-supported transparency and accountability of digital products, systems and services for the benefit of member states, citizens, society and economy (either demand or supply-side) and within the Rule of Law.
- **C. Objective: Interconnecting & Balancing Security Policies.** This mini-roadmap is envisioned to focus on how to introduce general security-

principles and generic cybersecurity controls and measures in horizontal regulations (such as the Cybersecurity Act (CSA) but also, Radio Equipment Directive (RED), General Data Protection Regulation (GDPR), General Product Safety Directive (GPSD), Machinery Directive, NIS Directive, eIDAS Regulation (EUid), Sales of Goods Regulations and the like), while avoiding overlap or at least avoiding conflicts between specific vertical regulations (such as for instance the Medical Device Regulation (MDR), regulatory standards such as the RTS of the Second Payment Services Directive 2 (PSD2) and many others), avoid conflicts, confusion or other discussion – and therefor delays in implementation and enforcement capabilities, as well as delay in building and achieving digital sovereignty – in the respective markets and between respective stakeholders on what applies, prevails, how to address conflicts, who is allowed to enforce what, et cetera.

8.3 Further Backgrounds regarding Legal & Policy Strategies

8.3.1 Making EU Regulations Fit for a Digital Sovereign Europe

Despite the indisputable benefits of the Digital Age for individuals, organisations of all sizes, member states, and society at large, Digital Age also raises risks, thus, surfacing aspects of critical importance within the Rule of Law outlined under Section 8.1, such as the complexity in attributing responsibilities.

In this context and bearing in mind how to best protect vital societal interests, the European Regulator has been quite active over the last years focusing on how to best protect the interests of individuals acting under multiple personas (e.g., data subjects, consumers), business interests of organisations (e.g., trade secrets) and interests of Member States, therefore, focusing -also- on how to best protect critical infrastructure (e.g., hospitals) and products (e.g., IoT devices).

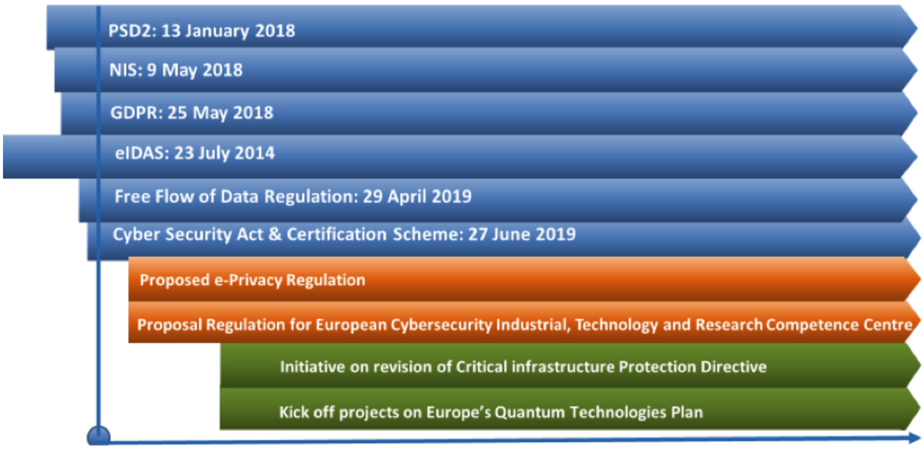

PSD2: 13 January 2018
NIS: 9 May 2018
GDPR: 25 May 2018
eIDAS: 23 July 2014
Free Flow of Data Regulation: 29 April 2019
Cyber Security Act & Certification Scheme: 27 June 2019
Proposed e-Privacy Regulation
Proposal Regulation for European Cybersecurity Industrial, Technology and Research Competence Centre
Initiative on revision of Critical infrastructure Protection Directive
Kick off projects on Europe's Quantum Technologies Plan

Figure 15: Digital & data regulatory landscape

Taking into account that the above figure produces merely an overview of the most relevant regulation at the EU level pertinent to the scope and the objectives of the present Roadmap, the discussion below provides the most up to date considerations regarding the status of implementation of GDPR, NIS, and CSA (cf. Deliverable D4.1 [82] and upcoming Deliverable D4.2, as well as in this Deliverable D4.4).

Making EU Regulations Fit for a Digital Sovereign Europe

May 25, 2020, marked the second anniversary of the application of Europe's General Data Protection Regulation which, as discussed in Chapter 4 of Deliverable D4.1 [82], was enacted to harmonise and strengthen the fundamental rights of individuals pertaining to the processing of personal data. The Communication published by the European Commission regarding the evaluation of the GDPR took into account input from the European Parliament, the European Data Protection Board, individual data protection authorities and other stakeholders [83]. As per the said report, the general view was that the GDPR was able to successfully achieve the objectives of strengthening individuals' right to personal data protection as well as guaranteeing the free flow of personal data within the EU, however, areas for future improvement were also identified.

In this Communication, the Commission highlights that while the GDPR provides for a consistent approach pertaining to data protection in the EU, it does give Member States discretion in certain areas. This has resulted in diverging approaches and fragmentation that has subsequently created challenges for conducting cross-border business, innovation, in particular as regards new technological developments and cybersecurity solutions. As a part of its action items necessary to support the application of the GDPR which is relevant for the purpose of this deliverable, the Commission has stated that it will support standardisation/certification in particular on cybersecurity aspects through the cooperation between the European Union Agency for Cybersecurity (ENISA), the data protection authorities and the European Data Protection Board.

NIS Implementation Status Update

The Directive on security of network and information systems (NIS Directive) aims at enhancing cybersecurity across the EU and is also the first piece of EU-wide cybersecurity legislation. The NIS Directive requires operators in critical sectors (such as banking, health, finance, transport) and enablers of information society services (such as app stores, social networks, and search engines) to implement effective risk management practices. It also requires Member States to set up at least one Computer Security Incident Response Team (CSIRT) that will be responsible for monitoring threats and incidents at a national level and to create appropriate response mechanisms. At an EU level, the Directive establishes a Network of the national Computer Security Incident Response Teams (the network of CSIRTs) to build trust and confidence between the Member States and enable effective communication.

Given that since its enactment in 2018, the cyber threat landscape has been constantly evolving and becoming more widespread, the European Commission published an initiative involving the review of the NIS Directive [84]. Based on evidence gathered, the Commission is of the view that while the NIS Directive immensely contributed to improving the cybersecurity capabilities within the Member States, there were various issues relating to its implementation.[85] Firstly, due to the minimum level of harmonization and the identification process applicable to operators of essential services, Member States have given a lot of discretion, which has resulted in fragmentation in the regulatory landscape and several inconsistencies [86]. This has also resulted in various sectors and actors with critical societal and economic activities and which are susceptible to cyber risks to be left outside the scope of the Directive. Hence, to achieve a 'Europe fit for the digital age' as envisioned by the EC, the Initiative aims to identify suitable policy options including non-legislative measures and possible regulatory interventions, as well as a combination of the two.

The EC recently sent out reasoned opinions [87] to Belgium, Hungary, and Romania referring to their failure to comply with their obligation set out in the Directive on security of network and information systems (NIS Directive). As per the NIS Directive, Member States were required to provide the Commission with information regarding the identification of operators of essential services in their respective jurisdictions, the deadline for which was 9 November 2018. For Belgium, identification of operators in critical sectors such as energy, transport, health, and drinking water supply and distribution is pending while Hungary is required to notify about the operators of essential services for the transport sector. Romania's authorities need to provide information on national measures allowing for the identification of operators, the number of operators of essential services, and thresholds used in the identification process. The Member States have been given two months to comply with their respective obligations.

Cybersecurity Act Implementation Update

In recent years, the EU has taken great strides to bolsters its resilience and its capabilities to identify, prevent, deter, and respond to cyberattacks and other malicious activities. The enactment of the EU Cybersecurity Act (CSA) in 2019 was one such initiative by the Commission to strengthen the EU Agency for cybersecurity (ENISA) and to create an EU-wide cybersecurity certification framework for digital products, services, and processes.

According to the CSA, ENISA also launched a month-long public consultation in July 2020 for the first candidate cybersecurity certification scheme, the Common Criteria based European cybersecurity certification scheme (EUCC). The EUCC scheme will replace the existing SOG-IS MRA and extend the scope to cover all EU Member States. To assist with this transition as well as to ensure consistent application of the CSA, the European Cybersecurity Certification Group (ECCG) was established. The ECCG comprises of representatives of national cybersecurity certification authorities or the representatives of other relevant national authorities.

ENISA has also set up a 15-member working group on Cybersecurity for Artificial Intelligence to advise ENISA on matters and developments relating to AI cybersecurity and to support ENISA in creating risk-proportionate cybersecurity guidelines for AI.

8.3.2 The Data Governance Act

On 25th November 2020, the European Commission published a Proposal for a Regulation on European data governance (Data Governance Act) [88]. The overarching objective of the proposal is to strengthen the availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU.

Data sovereignty as an essential component of digital sovereignty is well-represented in the Data Governance Act. For instance, the proposed Regulation introduces many measures to increase trust in data sharing, creates new EU rules on neutrality to reinforce the role of data intermediaries concerning data sharing, and provides for measures to facilitate the reuse of certain data held by the public sector. Moreover, the proposal facilitates companies and individuals to voluntarily make their data available for the wider common good under specific conditions.

The proposal is aimed to incentivise data sharing, especially in the public sector, thus fostering a culture, which is anticipated to encourage, without limitation, threat intelligence sharing, which is particularly relevant for the scope of CONCORDIA.

8.3.3 Making Contracts Fit for a Digital Sovereign Europe

Remark: This section is largely based on IERC Handbook 2017, Cognitive Hyperconnected Digital Transformation, IoT Standards Landscape – State of the Art, Analysis and Evolution, 2017, `https://doi.org/10.13052/rp-9788793609105`*, accessed Nov 27, 2020*

As mentioned earlier, cybersecurity relates to numerous layers including hardware, software, data, and service. This multi-layered structure often requires numerous different manufacturers and providers to participate, for example, in the manufacturing of a product, as well as in the provision of services during its lifetime. This setting accounts for a large number of contractual documents, licenses, notices, declarations, and/or reports to be in place and effective, not only between the supply-side actors themselves, but also vis-à-vis the customer. The resulting relationships tend to be very complex and bear a great deal of challenges in achieving transparency in allocating responsibilities and risks, as well as issues concerning jurisdiction and remedies.

One of the main challenges stakeholders with a role in the delivery of a system, product, or service is repeatedly faced with is the difficulty to understand applicable contracts, agreements, and other legal documents. Numerous reasons account for this issue, but for purposes of further discussion, it is mainly worth noting that, aside from the European versions of contracts often being verbatim reproductions of their US counterparts, (which may not be necessarily suitable), identifying all the applicable documents may be a challenge in itself. For example, in the case of Nest connected thermostat produced by Nest Labs owned by Google, this challenge is illustrated by about 13 legal documents which a user has to read to get a 'clear' picture of the rights, obligations, and responsibilities in the supply chain.

Having a clear picture of legal relationships is also challenging from the perspective of the scope of the documents. While they may claim that they are only applicable to one separate part of a product or service, in the Digital Age, it is difficult to imagine a part of the system or a separate layer functioning irrespective of the remaining parts or other layers, i.e. without affecting the whole ecosystem. However, to provide a sufficient amount of transparency and accountability, consumers and organisations (both private and public) must have an accurate and transparent account of how the layers (and the respective contractual documents) interact and who becomes relevant (not only active) in what layer. Just as the consumer or organisation should be able to identify the parties upon whom the service is dependent and who are the processors and sub-processors of data. Not only does this information provide the customer with greater transparency; it also helps them establish the extent of liability of various suppliers should a problem arise that requires legal redress.

Further questions concerning liability and other complex contractual issues arise in our Digital Era, for example, concerning the cybersecurity of IoT devices that can make autonomous decisions and enter into legally binding agreements with third parties (e.g., connected home appliances purchasing products from third parties). On the one hand, questions of liability for the actions of these autonomous devices are inevitable. On the other hand, although our traditional understanding of property is a static one, it will likely need to change and respond to the dynamic nature of IoT devices which can evolve and mature over time. Note that the latter has been taken into account by the European Regulator, who – in the context of the revision of the Product Safety Directive- provides for a new definition of ”product”.

From a separate perspective, it is also important to consider the status and the role of the customer in the ecosystem. It has been argued that two further distinctions of legal consequence can be made that are particularly relevant for consumers. 'First, the end-user may be the contracting customer or a third party, such as a family member. Second, the device itself may be owned by the customer or maybe leased to the customer by the supplier (or provided as part of rented or leased premises).' Considering the latter, 'the distinction between the device and the associated services becomes critical because the Nest Terms of Service states that if the device owner does not agree with the terms 'you should disconnect your products from your account and cease accessing or using the services'. However, in some jurisdictions, a disconnected IoT device would potentially breach the law. For example, according to the Sale of Goods Act 1979 of England and Wales, the purchasers of goods will 'enjoy quiet possession', which term would be potentially breached if when the Nest device was disconnected it loses most of its functionality.

Last but not least, complexities also arise in the context of clauses relating to the selection of jurisdiction in contracts. Most commercial contracts explicitly stipulate applicable law and jurisdiction governing them, to the maximum extent permitted by law. However, in cases where mandatory national laws apply, judges will have to abide by those. As a consequence, cases may arise in which the judge will have to apply different pieces of legislation, for example, to the same product. Already in today's connected world, it is not difficult to imagine a scenario in which a Dutch customer uses a US-manufactured product during their holiday in Tunisia, where the product was purchased in Venezuela, consists of software running in Ireland and uses applications developed by a Chinese company. This presents a very complex setting where the judge is expected to decide, for example, on damages that occurred due to cybersecurity incidents, based on different pieces of legislation that are likely to apply concerning the acquisition and functionalities of a given product.

Based on the above, there are considerable limitations on whether contracts are fit, also, for effectively providing for cybersecurity in the Digital Age. Those considerations, therefore, stress the necessity to look into the role self-regulatory instruments may play in relation to the protection of products, systems, and services from cybersecurity threats.

8.3.4 Making Self-Regulatory Instruments Fit for a Digital Sovereign Europe

Within the Rule of Law as depicted earlier under Section 8.1, there are several legal and policy instruments shaping behaviour that are all meant to synergize to best protect individual and societal interests in practice. This entails that, for instance, European Regulations cannot provide guarantees in absolute for the protection of those interests, as there are inevitable occurring gaps and challenges at the level of implementation that, subsequently, render of key significance the complementing role of contracts and policy instruments, such as the codes of engagement. Commitment to the latter may, also, reveal – especially – the social corporate responsibility of organisations to run the extra mile, potentially, mitigating the uncertainties resulting from regulation.

An appropriate code of engagement to strengthen cybersecurity in the Digital Age entails utilizing all relevant concepts found in a regulation, contract law, and other policy instruments to best serve stakeholders' interests concerning the safeguard of cybersecurity while safeguarding the vital societal interests associated with cybersecurity. In this respect, a balanced approach underlying a code of engagement for cybersecurity presumes to abstain from overreliance on mandatory regulations, as these may be quite generic. Similarly, an effective code of engagement in the field of cybersecurity entails avoidance of overreliance on a single standard, as this would merely further foster the already existing market fragmentation linked to the use of standards. Moreover, a code of engagement relevant for cybersecurity in the Digital Age could exceed the limitations of contractual arrangements between two parties (as common agreements are signed and sealed), while in a multi-stakeholder environment that would lead to the creation of a massive amount of paperwork, red tape and delays hampering -inevitably- daily business activities. Finally, a code of engagement fit for the Digital Age along the lines discussed, would not set terms and conditions (T&C) or similar of one company or organisation, which probably is the larger, unfair one that is non-negotiable, or the one that one has not been able to read, or the one that is unilaterally changed to your detriment (so no freely contracted-out and no balanced relationship, while pushing all liability to another); on the contrary, it would consider the interests of the wider community of stakeholders possibly adhering to the said code of engagement[9].

Note that at the moment of the present deliverable, there is work conducted within the CONCORDIA project, led by the legal partner and the relevant technical partners, that is directed towards the creation of a code of engagement -specifically- addressing the matter of Threat Intelligence Sharing.

8.3.5 Making Internal Policies Fit for a Digital Sovereign Europe

As mentioned in Section 8.1, also, policies have a role to play within the Rule of Law. By putting forward specific approaches in their internal policies, organisations are in the position to play a critical role concerning how regulations, contracts, and other policy instruments are implemented in reality. In light of this and in line with the overarching objectives of CONCORDIA, this section argues that for internal policies to be Fit for the Digital Age, they have to address how employees behave, therefore, focusing -also- on skills development. To this end -and given the dynamic nature of the cybersecurity field-, it is deemed both necessary and appropriate that cybersecurity skills are developed and sharpened in parallel in three layers, namely, at an individual level, at an organisational level, and a community level. Taking, also, into account that community building per se is addressed under Chapter 10 of the present Roadmap, the discussion below addresses skills in relation to the first two layers, meaning, at an individual level and an organisational level.

Skills at an individual level

Taking into account the work conducted under T3.4 and, in particular, the findings captured under the post-workshop report of CONCORDIA Workshop on Education for cybersecurity professionals, which took place in June 2020, internal policies could provide for the separate role of the Cybersecurity Consultant. This role has been internationally identified, but there is a lack of a concrete definition of the profile in all identified frameworks. Notably, in the related survey that was conducted under T3.4 the acquisition of a basic understanding of the legal aspects

[9] More information on a Code of Engagement for IoT, see CREATE IoT H2020 Project, Deliverable 05.01 IoT Policy Framework, european-iot-pilots.eu, accessed Nov. 27, 2020

of cybersecurity was considered as a key element of the Cybersecurity Consultant profile.

Furthermore, taking also into account the findings of a relevant JRC report [89], it is recommended that Cybersecurity Consultant professional has a basic understanding of the fundamentals of each cybersecurity domain identified, namely, on Assurance, Audit, and Certification, Cryptology (Cryptography and Cryptanalysis), Data Security and Privacy, Education and Training, Operational Incident Handling and Digital Forensics, Human Aspects, Legal Aspects, Theoretical Foundations, Identity and Access Management (IAM), Security Management and Governance, Network and Distributed Systems, Security Management and Governance, Software and Hardware Security Engineering, Security Measurements, Trust Management, Assurance, and Accountability.

In-depth knowledge of a certain domain will -naturally- depend on each professional's background and working experience..

Skills at an organisational level.

Although in practice this is hardly the case, there is a wide consensus in theory that cybersecurity should not be dealt with in splendid isolation within organisations. On the contrary, several departments should be involved and different levels of the hierarchy engaged. In this spirit, the ENISA report 'Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity' [90] provides a set of specific recommendations relevant for certain functions within an organisational structure, as illustrated in Figure 16.

With respect, the skills development, the present input to the Roadmap endorses the specific recommendations listed for each function addressed in the above-mentioned report, including, those pertaining to the role of soft skills. The latter could act as a catalyst, especially with respect to the effectiveness of cybersecurity practices.

Based on the earlier discussion and given the challenges raised by the dynamic nature of cybersecurity, internal policies of organisations to best provide for how regulations, contracts, and other policy instruments are implemented in practice could put special focus on skills development. It is of significance that the development of skills is seen both in micro-scale (on an individual basis), but also in macro-scale (based on the organisational structure).

8.4 Roadmap for Legal and Policy

The visualized current roadmap for research and innovation is shown in Figure 17.

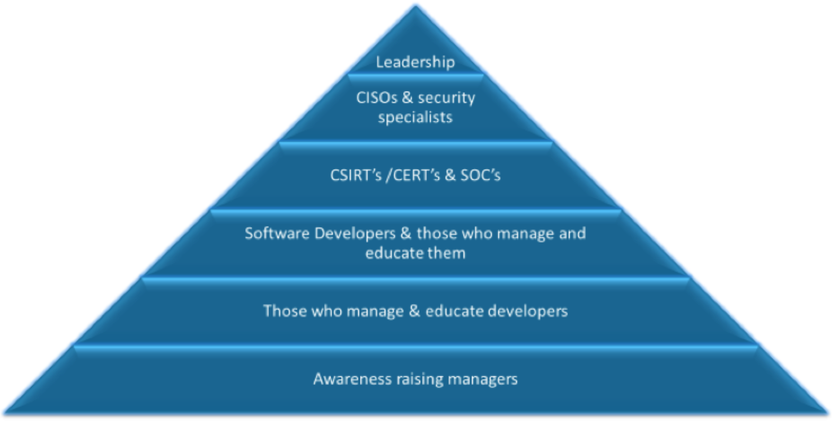

Leadership
CISOs & security specialists
CSIRT's /CERT's & SOC's
Software Developers & those who manage and educate them
Those who manage & educate developers
Awareness raising managers

Figure 16: Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity

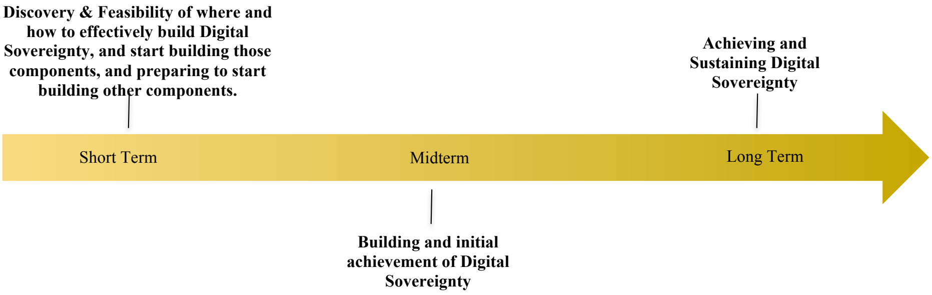

Discovery & Feasibility of where and how to effectively build Digital Sovereignty, and start building those components, and preparing to start building other components.
Achieving and Sustaining Digital Sovereignty
Short Term
Midterm
Long Term
Building and initial achievement of Digital Sovereignty

Figure 17: Overview from a Legal and Policy perspective of most important directions, steps, and threats for short-, mid-, and long-term timelines

9 Roadmap for Standardization and Certification

9.1 Standardization

The International Organisation for Standardization (ISO) defines an international standard as a document containing practical information and best practice. It often describes an agreed way of doing something or a solution to a global problem [91].' Standardization or standardisation is the process of implementing and developing technical standards based on the consensus of different parties that include firms, users, interest groups, standards organisations, and governments [92].

Standards play a paramount role in the dispersion of knowledge and innovation and development. Or as expressed by relevant studies, 'The processes for gaining this knowledge are at the heart of a standardization effort and the associated innovation outcomes.' 'there is a contingency relationship between standardization, search, and innovation outcomes, where one size does not fit all.' [92]

As stated by Mr. Peteris Zilgalvis, Head of Unit, Digital Innovation and Blockchain at DG CONNECT European Commission, 'Standards are an essential part in achieving the goals of Green Transition and Digital Sovereignty'. [10]

The European Union has created and published a Rolling Plan for ICT Standardisation. This Rolling Plan 'provides a unique bridge between EU policies and standardisation activities in the field of information and communication technologies (ICT). This allows for increased convergence of standardisation makers' efforts towards achieving EU policy goals [92].' Within this Rolling Plan, standardization actions have been identified also in the area of Cybersecurity. The actions and recommendations presented in this document take into account this Rolling plan as well as various plans, frameworks, and actions proposed by other organisations such as IEEE, ISO, CEN/CENELEC or ENISA.

9.1.1 Challenges

From the certification and standardisation perspective, currently, the following challenges have been identified.

Challenge 1: A common (accepted) terminology and language

As mentioned in the Scientific Opinion 02 of the High-Level Group of Scientific Advisors on Cybersecurity in the European Digital Single Market 'Cybersecurity combines a multiplicity of disciplines from the technical to behavioral and cultural. Scientific study is further complicated by the rapidly evolving nature of threats, the difficulty to undertake controlled experiments, and the pace of technological change and innovation. In short, Cybersecurity is much more than a science.'

In response to this fact, the European Commission has published a Proposal for a European Cybersecurity Taxonomy, to 'align the Cybersecurity terminologies, definitions and domains into a coherent and comprehensive taxonomy to facilitate the categorisation of EU Cybersecurity competencies.' [93]

Until recently (and in some cases even today) a globally accepted and standardized definition of Cybersecurity and a clear identification of its domain of development and application had not been implemented. The Proposal for a European Cybersecurity Taxonomy provides a taxonomy and a set of definitions regarding the Cybersecurity domain so that (amongst others):

- All interested parties, all relevant initiatives, and activities can have a common point of reference and a common language
- International Cybersecurity standards can have a common basis

To this last point, and to make sure that a strong basis exists to support the relevant standardization activities, this taxonomy should evolve:

- from a static three-dimensional model to a full range dynamic network and

[10] https://youtu.be/FtxWj0qtpBw, accessed Nov. 24, 2020

- to define and refine the definitions of other specific subdomains.

This effort should be systematic, with an increased audience and stakeholder involvement so that it becomes a true tool and guide, that will keep the pace of the fast evolution of the digital world. Currently, this challenge is under investigation and development and related recommendations are anticipated to be included in further detail in subsequent Roadmap editions.

Challenge 2: Low awareness and utilization of Cybersecurity Standards

'Standardization is one of the tools that can be applied to the continuous improvement of the organisation. Standardized work is one of the most powerful but least used lean tools.' [94]

'Though important, ICT standardization and its methods remain a topic that is not easily accessible. It seems that this field is becoming increasingly limited to the expert and remains mysterious to the non-expert.' [95]

During the last few years, initiatives have been undertaken to enhance, organise, fund, and coordinate ICT standardization. Although Cybersecurity originally belonged to the ICT domain, due to the increased complexity, variety and specialization, and consequences it has in daily life, society, and economy, dedicated effort should be given to the Cybersecurity Standardization aiming to the following:

- Awareness and Education on Cybersecurity standardization. Through these actions, it would be possible to educate the general public and the various interested parties regarding the ongoing standardization activities and also create a new generation of professionals that would be willing to work within and contribute to Cybersecurity standardization
- Funding for Cybersecurity standardization activities. Funding should be provided to facilitate the contribution to the Cybersecurity standardization activities.
- Inclusiveness in Cybersecurity standardization activities. Initiatives should be implemented so that there is no bias or barrier to the contributing professionals (sex, origin, religion, physical abilities, background, etc.).
- Open Standard Contributions to representatives from all types and sizes of organisations including micro, small and medium enterprises.
- Support the adoption of Cybersecurity standards by making them affordable and by creating an alignment between legislative and regulatory actions and the relevant standards.

Challenge 3: A lot of work to be done

As mentioned before the Cybersecurity domain is complex and has a high variety of domains and subdomains. This complexity is also inherited to and amplified in the standardization area.

Taking as a starting point one of the possible combinations of the taxonomy proposed within the Proposal for a European Cybersecurity Taxonomy [93]:

- Technologies and Use Cases: Cloud, edge and virtualization
- Data Security and Privacy: Research Domains
- Sectors: Financial

A high number of possible standards could be created and applicable in just this one combination. The standards could be generic or could be highly technical focusing on one characteristic of technique used in cloud implementations.

There are many Standard Developing Organisations (SDOs), but there is no hierarchical relationship, and may find themselves at a given time investing efforts is overlapping activities. This would not be avoided from an economical point of view but also because these duplications would lead to a fragmentation of the market and a decrease of the value of the resulting standards.

Standardization activities should be coordinated centrally, should allow for a collaboration, contribution and peer review between the SDOs and should allow for a variety of SDOs to be involved, in order to cover at the same time a high number of standards.

Challenge 4: Keeping up with evolution

Within the Threat Landscape of this document, the dimensions and evolution of Cybersecurity are presented. Moreover, the impact of the COVID-19 on the threats and the Cybersecurity domain is depicted. This information underlines the fact that Cybersecurity is a constantly evolving dynamic domain in need of constant overview, adaptation, and discovery.

This dynamic nature of Cybersecurity should also be reflected in the standardization activities and outcomes. Taking into account that standards are a result of consensus and multiple party contribution (taking from one to five years to complete), a very real danger, especially for the more technical standards, is for them to get deprecated, surpassed by current technology, and lose their value.

Some related recommendations that should be taken into consideration are:

- For Cybersecurity standards to reach their goals of usefulness and adoption, the
    - Cybersecurity standardization processes should be:
    - included in research activities as early as possible
    - realized in a ‘leaner’ way, allowing for at least initial versions of the standards to be available to a larger audience at an earlier time
    - coordinated and aligned every year. A Cybersecurity standardization plan should be established that will be regularly updated allowing for the changes in technology or situation to be adopted.
- The Cybersecurity standardization plan should incorporate standardization efforts that would be implemented, in alignment with the strategic goals of the industry in the following areas:

  - Compatibility / interoperability
  - Minimum Cybersecurity (Baseline)
  - Informative
  - Variety-reducing

In the document Understanding ICT Standardization: Principles And Practice [95], the above types of standards are presented along with their economic effects. An adaptation of this information to the Cybersecurity domain provides the following definitions:

Compatibility/Interoperability Standards

’A key role of standards is to ensure compatibility, which according to ISO 25010 consists of two components: coexistence and interoperability. Coexistence means that an IT service/product shares a common environment as well as resources with other independent services/products without adverse side effects, whereas interoperability is the ability of components to work constructively with one another. In the ICT sector, compatibility/interface standards play a crucial role.’

Within the cybersecurity context interoperability could be defined within the following two axes:

- The ability to have a selected security profile that is shared (communicated) between the various components of the system (e.g., a network)
- The sharing of Cybersecurity information, the ability to participate in threat-sharing communities or intelligence groups, and the analysis and evaluation of such solutions.

Elements of standardization belonging to this type are:

- Threat intelligence/threat information sharing
  - Interoperability maturity model standard that will guide stakeholders towards the development of interoperable CTII sharing solutions, or the adaptation of their existing ones. Improving the interoperability of cybersecurity information sharing will facilitate more effective protection against cyber threats in the future.[96]
  - Threat data standard that will facilitate the exchange between different platforms, communities, organisations, and systems.
  - DDoS clearing house / DDoS information exchange
- IoT
  - Secure communication standard for IoT. ‘Achieving interoperability is vital for interconnecting multiple things together across different communication networks. It defeats the purpose to have billions of sensors, actuators, tiny and smart devices connected to the Internet if these

devices cannot actually communicate with each other in a way or another.' [97] To this we need to add that this communication should follow the basic Cybersecurity principles ensuring confidentiality and integrity as needed.

- Training/cyber ranges
  - Cyber ranges scenarios standard to facilitate the sharing, reusing, and wider adoption of practical cyber range assisted education, training, and awareness.

Minimum Cybersecurity (Baseline)

Minimum Cybersecurity standards refer to standards containing a set of minimum acceptable security level requirements. These standards when implemented for processes, products, services and organisation would aim in:

- Reducing the level of risk felt by byers of the service / product
- Increasing the transparency within the market
- Increasing awareness within the market
- Reducing the level of uncertainty for the implementor
- Establishing a minimum level of security per product / service / process / organisation type

The last few years, as shown also in the Legal and policy issues section of this document, a number of legislative and regulatory initiatives have been implemented (e.g., GDPR, NIS, eIDAS, EU CSA etc) that require Cybersecurity measures to be implemented. Although the requirement and aim is clearly stated and understood, their majority does not provide information or guidance regarding how to achieve them.

Moreover, existing popular 'de facto' information security standards like ISO 27001, has been designed to provide a risk-based framework for managing information security, without being able to provide specifics.

All the above lead to implementation uncertainty, zero transparency and an unknown status regarding security.

Elements of standardization belonging to this type are:

- Baseline security standard (with minimum sets of controls) per industry
- Baseline security standard (with minimum sets of controls) for SMEs
- Baseline security standard (with minimum sets of controls) as part of the NIS directive implementation
- Security Maturity model standards that would allow for organisations to identify their security level,

while also guiding them regarding possible actions for improvement.

Standards of this type would need to cover all the issues discussed within this document including: 5G, Quantum, IoT, AI, Remote control Systems, Virtual and Augmented reality, Remote working, Autonomous driving, Secure Coding, Security and Privacy by Design, Security and Privacy by Default, Blockchain, Distance learning, and Cloud Computing.

Also, standards of this type could also cover issues mentioned above within a specific sector: E-health, Maritime, Transportation, Railway, Telecommunications, Financial, Insurance, Healthcare, and Services.

Informative 'Information and measurement standards contain codified knowledge and product descriptions. They constitute an important instrument for technology transfer, as they codify the work and experience of generations of experts in their specific fields, and support the dissemination of best practices. As such, they have a positive effect on the market by diffusing knowledge'.[95]

These standards would provide information regarding the various research domains and the technologies and use cases of cybersecurity. Within these standards, all interested parties would be able to retrieve knowledge regarding these areas, from the theoretical background, to the implementation techniques.

Elements of standardization belonging to this type are:

- Standards describing Risk Management frameworks
- Standards describing the establishment of relevant Management Systems
- Standards containing information on security controls principles and implementations without predetermining specific software or hardware solutions (e.g. Virtualization or VPN)
- Standards containing security assessment methods

Standards of this type would need to cover all the issues discussed within this document including: 5G, Quantum, IoT, AI, Remote control Systems, Virtual and Augmented reality, Remote working, Autonomous driving, Secure Coding, Security and Privacy by Design, Security and Privacy by Default, Blockchain, Distance learning, and Cloud Computing.

Also, standards of this type could also cover issues mentioned above within a specific sector: E-health, Maritime, Transportation, Railway, Telecommunications, Financial, Insurance, Healthcare, and Services.

Within the Cybersecurity domain, variety reducing standards would allow for the existence of components with specific security characteristics. These components could be physical, virtual or even human.

Elements of standardization belonging to this type are:

- Standards containing minimum competency definitions per Cybersecurity professional Role. This implementation would allow for equivalent systems of education, training and professional certification to be developed from different parties, in different parts of the European Union.

- Standards containing minimum characteristics for IoT devices allowing for a minimum level of security and communication.

Standards of this type would need to cover all the issues discussed within this document including: 5G, Quantum, IoT, AI, Remote control Systems, Virtual and Augmented reality, Remote working, Autonomous driving, Secure Coding, Security and Privacy by Design, Security and Privacy by Default, Blockchain, Distance learning, and Cloud Computing.

Also, standards of this type could also cover issues mentioned above within a specific sector: E-health, Maritime, Transportation, Railway, Telecommunications, Financial, Insurance, Healthcare, and Services.

9.1.2 Short-Term Aims

SA#	**Activitiy**
SA1	Development and evolution of a common (accepted) terminology and language
SA2	Funding of Cybersecurity standardization activities.
SA3	Inclusiveness in Cybersecurity standardization activities.
SA4	Open Standard Contributions to representatives from all types and sizes of organisations including Micro, small and medium enterprises.
SA5	Create a consolidated plan for European Cybersecurity Standardization and delegate responsibilities and authorities for standards development to a variety of organisations.
SA6	Include Cybersecurity standardization processes in research activities
SA7	Implement a leaner and more open process of Cybersecurity Standardization
SA8	Create a Secure communication standard for IoT
SA9	Cyber range scenarios standards
SA10	Minimum Cybersecurity standards for IoT
SA11	Minimum Cybersecurity standards for Cloud Computing
SA12	Minimum Cybersecurity standards for distance working
SA13	Cybersecurity Skills framework
SA14	Standards regarding auditing / assessment methodologies for cybersecurity products
SA15	Standards regarding end to end testing of systems and services
SA16	Security verification and security assessment/testing standards for new protocol/network specifications

9.1.3 Mid-Term Aims

SA#	**Activitiy**
SA17	Awareness and Education on Cybersecurity standardization.
SA18	Support the adoption of Cybersecurity standards by making them affordable and by creating an alignment between legislative and regulatory actions and the relevant standards.
SA19	Implement Threat intelligence / threat information sharing related standards
SA20	Minimum Cybersecurity standards for SMEs
SA21	Minimum Cybersecurity standards for Critical infrastructure
SA22	Minimum Cybersecurity standards for Remote control Systems
SA23	Informational Standards for Security and Privacy by Design
SA24	Informational Standards for Security and Privacy by Default
SA25	Standards for Cybersecurity Education
SA26	Minimum security standards for cybersecurity products (in relation to the CSA)
SA27	Minimum baseline security and privacy requirements for the Aerospace Sector – with contextual risk- and impact-based measures added where appropriate – for easy and consistent implementation

9.1.4 Long-Term Aims

SA#	Activitiy
SA28	Minimum Cybersecurity standards for Quantum
SA29	Minimum Cybersecurity standards for 5G
SA30	Informational Standards for different industries
SA31	Standards for other areas: AI, Virtual and Augmented reality, Autonomous driving, Blockchain
SA32	Standards for principle-based, risk- and impact based, human-centric continuous assurance for the security of critical infrastructures.

9.2 Certification

Certification is the third-party attestation related to products, processes, systems or persons. Whereas attestation, is issue of a statement, based on a decision following review, that fulfillment of specified requirements has been demonstrated. Certification can apply to a product, process, system, person or body. Depending on the subject of certification, different international standards provide the related best practices (e.g., ISO 17021, ISO 17024 or ISO 17025).

The Cybersecurity Act (hereinafter CSA) entered into force in June 2019 with a view to bring together the current Cybersecurity certification activities and policies across the Member States. The CSA follows an array of legal instruments that compose the legal framework of the Digital Single Market while benefiting from the framework on standardisation, laid out by means of Regulation (EU) 1025/20123, and provisions on conformity assessment, laid out in Regulation (EC) 765/20084.

The CSA is a multi-layered regulation that on the one hand addresses the updated ENISA mandate and, on the other, lays out the EU Cybersecurity certification framework. ENISA is tasked with a new competence, namely to prepare candidate Cybersecurity certification schemes. Thematic application areas likely to be affected by the Cybersecurity certification provisions of the CSA may include specific ICT products (e.g., semiconductors), services (e.g., cloud services) and processes (e.g., information security related methods).

The mission of ENISA in the area of the EU Cybersecurity certification framework is outlined as follows: 'To pro-actively contribute to the emerging EU framework for the ICT certification of products and services and carry out the drawing up of candidate certification schemes in line with the Cybersecurity Act, and additional services and tasks'.

To the above-mentioned vision and scope of Cybersecurity of the CSA, the certification of Cybersecurity skills and organisations should be added.

The meaning of cybersecurity certification per element is:

- For products
  - that products have been tested based on approved and appropriate methods
  - that products fulfil specific cybersecurity requirements
  - that products are achieving a specific level of assurance (e.g., basic, substantial and/or high)
  - that the cybersecurity risk of using a specific product is of the equivalent value (e.g., basic, substantial and/or high)
- For services
  - that services have been designed and are operated according to specific Cybersecurity requirements
  - that services are achieving a specific level of assurance (e.g., basic, substantial and/or high)
  - that the Cybersecurity risk of using a specific service is of the equivalent value (e.g. ,basic, substantial and/or high)
  - that the services have been audited based on approved and appropriate methods
- For processes
  - that processes have been designed and are operated according to specific Cybersecurity requirements
  - that processes are achieving a specific level of assurance (e.g., basic, substantial and/or high)
  - that the Cybersecurity risk of operating a specific process is of the equivalent value (e.g., basic, substantial and/or high)
  - that the processes have been audited based on approved and appropriate methods
- For skills
  - that specific Cybersecurity competence requirements have been identified per relevant Role
  - that the skills have been assessed based on approved and appropriate methods
  - that the competence of thus assessed individual is appropriate to the specific Role
- For organisations

  - that the organisation has designed and implements a system for the management of its Cybersecurity posture based on specific Cybersecurity requirements
  - that the organisation is achieving a specific level of assurance (e.g. basic, substantial and/or high) through this implementation
  - that the Cybersecurity risk for this organisation is of the equivalent value (e.g., basic, substantial and/or high)
  - that the organisation has been audited based on approved and appropriate methods

When considering Cybersecurity certification, the following key benefits are identified:

- Certification enhances the ability of consumers and European Member States governments to acquire more cybersecure ICT products, services and processes.
- Certification provides a relative transparency regarding the level of assurance of the product, service or process being acquired.
- Certification allows organisations or governments to select the level of risk they will be exposed to by selecting the product / process / service of the respective level of assurance
- Certification allows for better comparison between different vendors
- Certification allows for circulation of products / services from a multitude of providers

The key challenges for Cybersecurity certification are market fragmentation and uncertainty with regard to the assurance provided by existing arrangements and schemes.

To minimize these risks, ENISA is envisioned to play the leading role in the certification ecosystem and coordinate the relevant activities.

As stated in the CSA, (Article 47) ‘The Commission shall publish a Union rolling work programme for European Cybersecurity certification (the Union rolling work programme) that shall identify strategic priorities for future European Cybersecurity certification schemes. The Union rolling work programme shall in particular include a list of ICT products, ICT services and ICT processes or categories thereof that are capable of benefiting from being included in the scope of a European Cybersecurity certification scheme [98]! The first version of the Union rolling work programme for European Cybersecurity certification was expected to be published on the 28th of June 2020 but has been delayed. [It is expected to be published within 2020]. At the same time the first two Cybersecurity certification initiatives has started under ENISA's coordination.

There are:

- The EUCC scheme (Common Criteria based European candidate Cybersecurity certification scheme) and it looks into the certification of ICT products Cybersecurity, based on the Common Criteria, the Common Methodology for Information Technology Security Evaluation, and corresponding standards, respectively, ISO/IEC 15408 and ISO/IEC 18045. [99]
  - The document is currently under deliberation having completed its 1st public consultation at the end of July 2020
- The Cloud computing scheme. Acting on a prominent Commission initiative, dubbed CSP-CERT, representatives of both the private and the public sectors have already reached consensus and put forward a proposal for a certification scheme for the cloud; however, several aspects have yet to be sorted out. The Commission request to ENISA concerning a Cybersecurity certification scheme for Cloud services has been grounded on the Regulation for the free flow of non-personal data. Other relevant aspects concerning the Cybersecurity of non-personal as well as personal data flows are likely to also come under the scope. [100]

9.2.1 Challenges

Certification is a maturity action and as such several steps including development and standardization have to be completed before it is realized.

ENISA as key role

As mentioned above, ENISA is playing a key role in the design, implementation, approval and monitoring of the Cybersecurity schemes under the CSA. This by itself is a huge undertaking creating a bottleneck to the development process. At the same time, there is an increasing need from the market for guidance and support regarding Cybersecurity certification. As time goes by, more schemes will be created that will have a specific audience and recognition, leading to a market fragmentation and devaluation of certification. It is important especially for the circulation of products and services within the European Union that each country / vendor does not create a dedicated certification scheme, leading companies targeting multiple markets to have to comply many times to different or partially overlapping or even conflicting requirements. To address this challenge, the task of creating an acceptable set of requirements and relevant certification schemes should be spread to the different stakeholders, allowing for fast and concurrent development in multiple areas.

Cybersecurity Re: Privacy

Privacy has been a rising concern globally and in particular within the European Union after the activation of the GDPR. Putting it in simple terms, to make sure that personal information is protected also against threats to the confidentiality, integrity and availability of this information need to be implemented. Part of these measures are measures that would be implemented also from a Cybersecurity point of view. This apparent connection between these two terms, indicates that possible solutions of the one domain should take into consideration the other domain also. In Article 42 of the GDPR, relevant certification schemes are introduced which will be voluntary, transparent and approved by the relevant competent authorities (for National ones) and the European Data Protection Board (for European wide certification schemes). It would be useful, since such schemes have not been completed yet, to have an integration with the applicable Cybersecurity ones, so that more transparency and simplicity exists in the market.

The areas where Cybersecurity certification is needed are mentioned below (as a summary) and they are split based on the implementation timeline in the following section:

- Network devices,
- Storage devices,
- 5G,
- e-health devices,
- Services under the NIS,
- Secure Coding,
- Security by design,
- Security by default,
- IoT,
- AI,
- Wearable devices,
- Robots,
- Hosting services,
- Teleconference,
- Remote working,
- Distance learning,
- Computer games,
- Elections,
- Shared Lab infrastructure,
- Blockchain,
- Proximity applications and devices,
- Bitcoin,
- Autonomous transportation, and
- Quantum.

The effect of COVID-19 on standardization and certification

As with all other aspects of life, standardization and certification has been influenced by the COVID-19 pandemic crisis. The rise of teleworking, distance learning and the genesis of proximity tracing systems has led to a shift in standardization towards these areas. Already, standards are being developed for the secure implementation of such systems and certification schemes should follow that would allow the consumer, organisations and governments to be able to gain a needed transparency to their cybersecurity posture.

9.2.2 Short-Term Aims

CA#	Activitiy
CA1	Spread the creation of requirements and relevant certification schemes to the different stakeholders, allowing for fast and concurrent development in multiple areas, based on a concrete certification plan
CA2	Create an accepted methodology for testing cybersecurity products and a central certification framework
CA3	Create a European Accreditation framework for the testing and certification of cybersecurity products, processes and systems
CA4	Create a European Accreditation framework for the testing and certification of the privacy of products, processes and systems
CA5	Certification of Product Security Incident Response Team (PSIRT) program for vendors to help their customers in addressing the security of their products in a prompt and efficient way
CA6	Cybersecurity certification scheme for IoT
CA7	Cybersecurity certification scheme for Network devices
CA8	Cybersecurity certification scheme for Cloud services
CA9	Cybersecurity certification scheme for Remote working

9.2.3 Mid-Term Aims

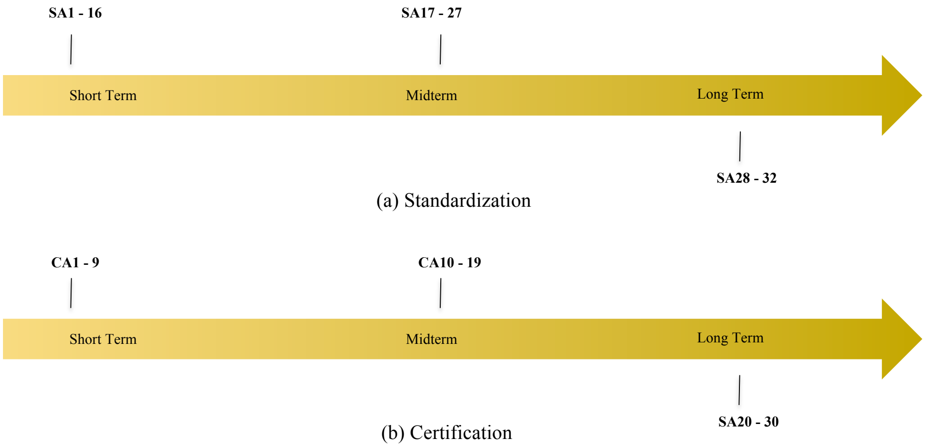
CA#	**Activitiy**
CA10	Computer games
CA11	Teleconference
CA12	Distance learning
CA13	Wearable devices
CA14	Hosting services
CA15	Security by design
CA16	Security by default
CA17	e-health devices
CA18	Storage devices
CA19	Cybersecurity capabilities in aviation certification procedures as well as an upgrade to the certification procedures in this area as well.

9.2.4 Long-Term Aims

CA20	Shared Lab infrastructure
CA21	Bitcoin
CA22	Autonomous transportation
CA23	Quantum
CA24	Blockchain
CA25	Elections
CA26	Robots
CA27	AI
CA28	Secure Coding
CA29	Services under the NIS
CA30	5G

9.3 Roadmap for Certification and Standardization

The visualized current roadmap for certification and standardization is shown in Figure 18.



(a) Standardization

(b) Certification

Figure 18: Overview from a Certification & Standardisation perspective of most important directions, steps, and threats for short-, mid-, and long-term timelines

10 Community Building

'If you want to go fast, go alone. If you want to go far, go together' is a famous universal wisdom.

The proposal for Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres [101, 102, 103, 104] is one of the excellent mission instruments, as for once it is designed to fragmentation and convert duplication of efforts to synergies of coordination and cooperation, including the ability to support various development of European cybersecurity competences and capabilities, also to help built, achieve and sustain digital sovereignty.

10.1 Hybrid Interconnected & Intertwined Ecosystem of Ecosystems

However, although the vision and mission are clear, and everybody agrees that collaboration is essential, the question how to collaborate is generally not addressed let alone operationalised. This, for instance, as per the multiple values, needs, interests, maturity levels, focus areas, each with their own short-term, mid-term and long-term characteristics and preconditions. Furthermore, the proposed Regulation will be focussing on four main domains that are intertwined per context, per addressed objective, stakeholders group, impact, challenge, opportunity and life cycle phase.

Those four main domains are already mentioned and visualised in Figure 19, being (i) Sovereignty & Collaborative Resilience, (ii) Economic Development & Competition, (iii) Research & Innovation, and (iv) Education, Skills & Jobs. These are intertwined as one affects the other, as one requires the other, and as one adds to and augments the other.

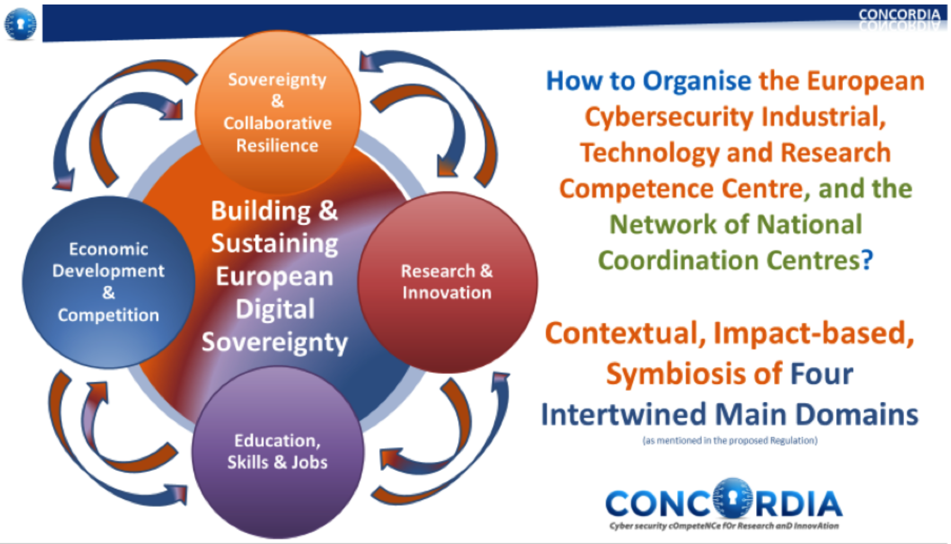
For purpose of the CONCORDIA Cybersecurity Roadmap for Europe, various objectives, challenges respectively scenarios regarding or related to most-notable community building strategies have been identified. Some of those are already highlighted below where others are merely mentioned yet under development in a stage that these are expected to be incorporated more extensively in the next edition of the Roadmap.

Hereunder, the currently identified objectives, challenges respectively scenarios (also collectively described as initial 'mini-roadmaps') are mentioned, each generally for local, sectorial, regional, member state, European Union team building, continuous improvement and sustainment of European digital sovereignty and the related intertwined four main domains and respective subdomains.

10.2 Objectives, Challenges & Scenarios

10.2.1 Objective: Know (Your Enemy and Know) Yourself

State of Play (SOP): As stated in the Commission Staff Working Document Impact Assessment related to the Proposal for Regulation establishing the European



CONCORDIA

Sovereignty & Collaborative Resilience

Economic Development & Competition

Building & Sustaining European Digital Sovereignty

Research & Innovation

Education, Skills & Jobs

How to Organise the European Cybersecurity Industrial, Technology and Research Competence Centre, and the Network of National Coordination Centres?

Contextual, Impact-based, Symbiosis of Four Intertwined Main Domains

(as mentioned in the proposed Regulation)

CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

Figure 19: Contextual, impact-based symbiosis of four intertwined main domains

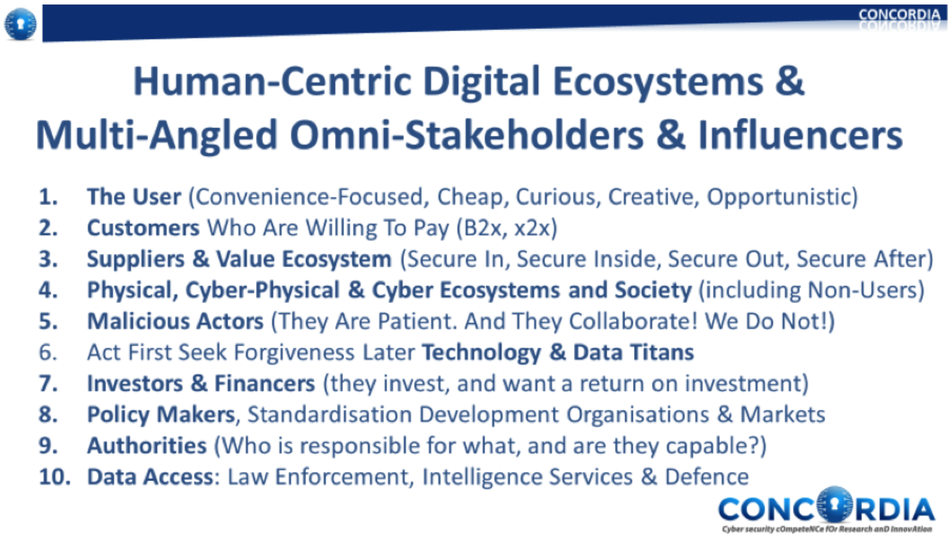
Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, as well as reconfirmed in June 2020 by the Council, Cybersecurity is an issue local, national and cross-border issue of common interest of the European Union, and it needs to make sure that it has the capacities to secure its economy, democracy and society. For Europe to be prepared it needs to have a thriving cybersecurity ecosystem, including industrial and research communities.

However, do we truly know the ecosystem and its communities, and do we and they know, understand and appreciate each others capabilities, experience, offerings, challenges and needs to build, achieve and sustain future-proof digital sovereignty?

Currently, one cannot represent that we really know ‘ourselves’ as existing European Union cybersecurity ecosystem and existing communities, also as cybersecurity is a vast and constantly evolving and expanding domain, horizontal and multifaceted dimension, which nowadays relevant almost in any sector, vertical, separate or converging markets and basically any part of society, economy and daily life.

State of the Art (SOTA): ‘If you know the enemy and know yourself, you need not fear the result of a hundred battles.’ is a famous quote allotted to Sun Tzu from his publication the Art of War.

The state of the art should be to know ‘ourselves’ as cybersecurity universe, know what and where our weakness and strengths are, who we are missing out of to complement and optimise. It should clear – and continuously challenged, updated and improved – what such cybersecurity ecosystem and its communities should consist of to build, achieve and sustain future-proof digital sovereignty, what and



CONCORDIA

Human-Centric Digital Ecosystems & Multi-Angled Omni-Stakeholders & Influencers

1. **The User** (Convenience-Focused, Cheap, Curious, Creative, Opportunistic)
2. **Customers** Who Are Willing To Pay (B2x, x2x)
3. **Suppliers & Value Ecosystem** (Secure In, Secure Inside, Secure Out, Secure After)
4. **Physical, Cyber-Physical & Cyber Ecosystems and Society** (including Non-Users)
5. **Malicious Actors** (They Are Patient. And They Collaborate! We Do Not!)
6. Act First Seek Forgiveness Later **Technology & Data Titans**
7. **Investors & Financers** (they invest, and want a return on investment)
8. **Policy Makers**, Standardisation Development Organisations & Markets
9. **Authorities** (Who is responsible for what, and are they capable?)
10. **Data Access**: Law Enforcement, Intelligence Services & Defence

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

Figure 20: Overview of different stakeholders and influencers of digital ecosystems

who we are missing in existing communities, how to complement and cater for a full-spectrum, intertwined, multi-tiered and multi-layered ecosystem.

The state of the art should include taking into consideration – on a scenario by scenario basis, respectively objective/challenge by objective/challenge basis – the numerous stakeholders that are either directly or indirectly part of (whether desired, knowingly or otherwise) any scenario respectively objective, challenge or other situation or case. Some examples of such stakeholders are set forth in the visual below (Figure 20). In each case, the landscape of the various relevant stakeholders and various influences each may of will have, will be different. Therefore, a contextual approach is pre-requisite.

GAP (SOTA -/- SOP): The basis query 'How', which is generally been mentioned as the current main challenge, the first part of the GAP actually starts with 'Who'. Based on that, one can identity, assess, discuss and organise what binds or could bind the member states – in all their various facets and in the various domains and sectors relevant for government and society – and its national stakeholders together, which is for the benefit of the member states as well as others – and therefor the European Union –, both top-down and bottom-up. Furthermore, as per the ever evolving and expanding domain that is or relates to cybersecurity and digital sovereignty, this will need to be a continuous effort.

Short-Term: For the Short-Term, bridging the initial main GAP cross-EU initiative is necessary to discover, identify, map and plot the various current and potentionally near-future and future stakeholders and their various interests, values, expectations and the like, including identity the various common grounds, benefits and preconditions each may foresee or seek for, either with scenario's and impact plotting or otherwise.

Mid-Term: For the Mid Term, insight and oversight will grow to a level (1) where European stakeholders that wish to actively contribute to European digital sovereignty can start to understand and appreciate each other, and (2) where scenarios can be operationalised, and deployed. Starting relatively modest yet in a way that has the ability to scale and agility to evolve and be improved is recommended. As appreciation within the EU is sought after, some traction and growth of the willingness to collaborate is expected to increase. Further organising, executing, monitoring and improving are essential.

Long-Term: Where not yet achieved in the Mid-Term, getting to know and appreciate the various European stakeholders, both locally, regionally, nationally and otherwise can be scaled in the Long Term. As mentioned, narrowing this will be a dynamic and ongoing effort that will need constant attention and agility.

Conclusion: Getting to know yourself is the first step to any next step. This is the way to start building trust, and thereafter add further trust layers on top of that. For all that we did not know before, we should not want to explain the notion of building, achieving and sustaining European digital sovereignty to them; they should understand it themselves. The above-mentioned proposed Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres offers a possibility to cater for such a meta-framework to take in the recommendation set forth above.

10.2.2 Challenge: Short-, Mid- & Long-Term Community Engagement

State of Play (SOP): Connecting and collaborating with each other sounds easy, including – seemingly – the start, yet it has probably one of the most underestimated and difficult things to achieve and sustain. One if the reasons, next to the objective set above in Section 10.2.1: ‘Know (your enemy and) know yourself’, is that the start looks so easy that the initial architecture, stakeholders and governance are generally too rigid, too centralised and not omni-stakeholder enough, where down the road it is impossible or nearly impossible to change let alone pivot and other improve. Another reason is that intentions and horizons tend to be dynamic and therefor subject to change, even those of the initial group of stakeholders, as well as for those stakeholders that generally appear on the horizon in the mid term and long term. Particularly in the cybersecurity domain and regarding digital sovereignty, this all in all is a challenging problem set.

State of the Art (SOTA): The state of the art could be that each and every stakeholder understands that there is no one solution, there is no one group with the answer, no one technical fixture, and that is this all about working together, as teams, to achieve outcomes. The state of the art is that this is a team sport of sports, and that each sport has its own rules of engagement, has its own particulars, needs its own capabilities, and diverse groups of people – both in the field and outside the field, and that each has different phases that requires different competences and capabilities.

GAP (SOTA -/- SOP): Part of the GAP is to have a mission-centric focus, while appreciating that the point on the horizon will never be met as a new horizon will appear while nearing the initial horizon. Based on this notion, one can reverse engineer how, with whom, and with what to manover towards the intended yet dynamic point on the then relevant horizon – which will probably not be lead to a navigation in a straight line –. With that, one can work to organising living labs (as well as field labs and otherwise) competence centers & deployable capabilities.

Short-Term: For the Short-Term, these are examples of topics to consider:

- Identify community and other stakeholders needs and expectations, from all perspectives, and in the various phases;
- Identity awareness, acceptance and adoption metrics and KPIs;
- Identify skills, capabilities and experience that can contribute best to individual's readiness for 21st Century interdisciplinary challenges;
- Engage a diverse group of individuals to take a 360-degree view;
- Stimulate collaboration, innovation and co-creation;
- Invest in technical and organisational skills and creation of more jobs that add value to society and economy, and digital sovereignty in particular;
- Develop human-centric technology by involving stakeholders and the community from the very beginning, and;
- Build trust and trustworthiness.

Mid Term: For the Mid-Term, these are examples of topics to consider:

- Creation of living labs and local, regional, national and (European) sectorial competence centers to attract diverse ideas and perspectives to relevant challenges;
- Start small scale pilots;
- Facilitate public participation to identify threats and vulnerabilities caused by use of certain technologies and processes;
- Devise innovative strategies and measures to counter potential threats and vulnerabilities;
- Strengthen capability building;
- Initiate medium-scale pilots that will include more than one member state;
- Identify skills and enhance participation from the additional member states;
- Identify and map the outcome, challenges, hurdles and interdependencies of small-scale pilot;
- Evaluate the takeaways, build on previous deficiencies and expand the results of small-scale pilots;

- Develop tailor-made solutions and strategies;
- Ensure seamless collaboration and communication in the region and beyond, and;
- Present results of pilots, needed skills and strategies to policy makers.

Long-Term: For the Long-Term, these are examples of topics to consider, where the focus is to expanding, sustaining and improving the various living Labs, competence centers and further capability building.

- Initiate large-scale pilots that will include all member states;
- Identify skills and enhance participation from all member states;
- Identify and map the outcome, challenges, hurdles and interdependencies of small-scale and medium-scale pilots;
- Evaluate the takeaways, build on previous deficiencies and expand the results of small-scale and medium-scale pilots;
- Develop tailor-made solutions and strategies;
- Ensure seamless collaboration and communication in the region and beyond, and;
- Incorporate results of pilots, needed skills and strategies to policies.

Conclusions: In most of the community building scenarios it is relevant to start in a diligent, mission- and principle-based yet solid way – without bias or assumptions –, and reverse-engineer how to complete the mission, how should be in the team, what does the team needs and how to distribute the contributions, work, risks, fruits and other benefits. Without team work, co-creation and co-allocation on a phase-by-phase basis one would miss out on a prerequisite success factor and main enabler and facilitator to build, achieve and sustain European digital sovereignty.

10.2.3 Other Objectives, Challenges or Scenarios

Other objectives, challenges or scenarios regarding community building are under investigation and development as a mini-roadmap, and are currently anticipated to reach a certain level of maturity and detail to be included in subsequent Roadmap edition(s), including the following:

- Objective: How to move from communities to a hybrid, interconnected and intertwined ecosystem of ecosystems? This mini-roadmap is envisioned to move beyond the generally fragmented, unconnected, unbalanced and incomplete communities towards hybrid interconnected hypercubed ecosystem of ecosystems, where those communities are part of but will learn to understand and appreciate the synergies and interdependabilities and merits of ecosystems;

- Objective: How to build a NSG Ecosystem of ecosystems? This mini-roadmap is envisioned to be built within the current framework of the propose Regulation mentioned in the introduction of this chapter. If will consider a hybrid, dynamic, distributed yet coordinated and transparent multi-layered meta-architecture of multiple communities in multiple ecosystems with an underlying European Union level ecosystem to enable and facilitate both digital sovereignty for member states, its citizens, society and other stakeholders as well as digital sovereignty for the European Union at large. This, included without limitation (i) Research & Innovation community building, (ii) Education, Skills & Jobs community building, (iii) Economic Development & Competition community building and, last but not least: (iv) Sovereignty & Collaborative Resilience community building, as visualised in Figure 19.
- Objective: Cybersecurity community building for, with and by EU periphery countries, regions and partners. This mini-roadmap is envisioned to enable the European Union, member states and other stakeholders to connect and collaborate with the periphery, as digital, cyber and related matters to not stop at the borders of the European Union and vice versa, and;
- Some objectives, challenges or scenarios that are defined elsewhere in this Roadmap, but then where relevant developed from the community building angle, such as for instance the objectives set forth in Section 8.2.1 (Trusted Experience Sharing), Section 8.2.3 (Member States NIS Directive Comfort & Capability Building), Section 7.2.1 (Landscaping H2020 Cybersecurity Deliverables, and Section 7.2.2 (Narrowing the Investment Gap), to name a few.

10.3 Roadmap for Community Building

The visualized current roadmap for research and innovation is shown in Figure 21.

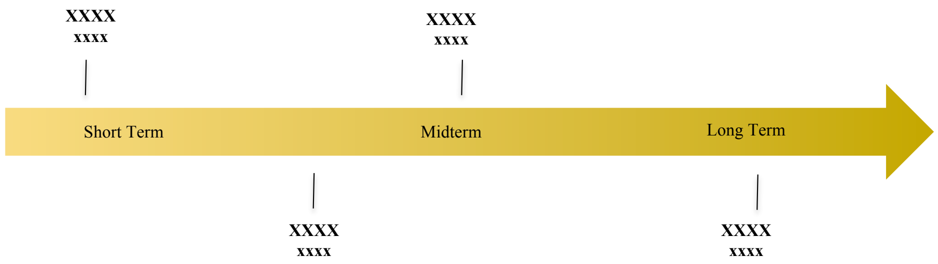


Figure 21: Overview from a Community Building perspective of most important directions, steps, and threats for short-, mid-, and long-term timeline

11 Other Aspects: Sustainable/Green ICT

(Will be worked on in 2021)

A holistic approach to the specification of the Cybersecurity Roadmap includes other aspects such as green technology and sustainability. Global dependence on renewable energy sources has increased steadily over the last years. We have two sides of a medal. On one side, energy companies are under threat from national-states, malicious attackers. On the other side, data centers use an estimated 200 Terawatt hours each year. Our digital society is very data-hungry and energy-consuming. Sustainable ICT involves the use of ICT equipment that requires fewer materials, less energy and less waste. Cybersecurity Roadmap for Europe needs to address such aspects as well, especially with the goal of the European Green Deal.

12 Interdependencies Between Roadmaps

(Will be worked on in 2021)

13 Conclusions

The current preliminary version of the Deliverable D4.4 documents the work on the CONCORDIA's Cybersecurity Roadmap for Europe up to 12th of December 2020. It is a living document and will be updated until the end of the project.

CONCORDIA advocates to take a holistic approach in the specification of the Roadmap for Cybersecurity. The limitation only on the technological (research and innovation) aspect is not an adequate approach with respect to the overall goal of achieving European digital sovereignty. Technology cannot be observed independently of people, economics, legal and certification as well as standardization aspects.

On cybersecurity, digital sovereignty and policy strategies regarding connected devices, the Council of the European Union recently nicely highlighted it as follows: '... that the European Union and its Member States need to ensure their digital sovereignty and strategic autonomy, while preserving an open economy. This includes reinforcing the ability to make autonomous technological choices and as one of the main pillars, resilient and secure infrastructures, products and services for building trust in the Digital Single Market and within the European society. The European Union's core values preserve in particular privacy, security, equality, human dignity, rule of law and open Internet as prerequisites for reaching a digital-driven human-centric society, economy and industry'.[11]

As the Deputy Secretary General of NATO, Mr. Geoană, put it: 'Our societies have to be tech ready, and our tech sector security ready. Our open democracies, educational models – they all bring levels of creativity and disruption that other forms of government cannot. Large companies compete with start-ups to generate fresh thinking. This drives innovation, encourages healthy competition, and builds societal resilience'.[12]

CONCORDIA identifies six dimensions of observation. For each dimension a separate roadmap is proposed. Since the six dimensions are intertwined and have interdependencies, this is true also for the roadmaps. All activities in the roadmaps are structured on a time scale into short-, mid- and long-term activities.

The discussion starts with an analysis of the current threat landscape and the identified recommendations, also ranked according short-, mid- and long-term scale. CONCORDIA identifies the following roadmaps: (i) Roadmap for Research and Innovation, (ii) Roadmap for Education and Skills, (iii) Roadmap for Economics, (iv) Roadmap for Investments, (v) Roadmap for Legal and Policy, (v) Roadmap of Standardization and Certification and (vi) Roadmap for Community Building. Since cybersecurity is the pillar of our digital society, other aspects such as sustainable ICT or cybersecurity and green technology will be addressed in the next years. The interdependencies between roadmaps will be addressed in the next years, too.

[11] Council, 2 December 2020, Cybersecurity Connected Devices, https://data.consilium.europa.eu/doc/document/ST-13629-2020-INIT/en/pdf

[12] NATO Deputy SG, 25 November 2020: https://www.nato.int/cps/en/natohq/news_179709.htm

14 Acronyms

AI	Artificial Intelligence
API	Application Programming Interface
ATI	Assistance Technique Industrielle
BEC	Business Email Compromise
CaaS	Cybercrime as a Service
CAPEX	Capital Expenditure
CASB	Cloud Access Security Broker
CERT	Certificate
CI/CD	Continuous Integration & Continuous Deployment
CIA	Confidentiality, Integrity, Availability
CNI	Critical National Infrastructure
CPC	Consumer Protection Cooperation Network
CPS	Cyber Physical System
CPU	Central Processing Unit
CSA	Cybersecurity Act
CSC	Cybersecurity Culture
CSEM	Child Sexual Exploitation Material
CSIRT	Computer Security Incident Response Team
CSP	Cloud Service Provider
CV	Curriculum Vitae
DoA	Description of Action
DDoS	Distributed Denial of Service
DevSecOp	Development, Security, Operations
DNS	Domain Network System
DoH	DNS over HTTPS
DoS	Denial of Service
DTLS	Datagram Transport Layer Security
DX.Y	Deliverable DX.Y
EC	European Commission
EDSC	European Digital Skills Certificate
EIC	European Innovation Council
ELLIS	European Laboratory for Learning and Intelligent System
ENISA	European Network and Information Security Agency
EU	European Union
EUCC	European Cybersecurity Certification Scheme
EUCG	European Cybersecurity Certification Group
FUD	Fear, Uncertainty, and Doubt
GDPR	General Data Protection Regulation
GPRS	General Packet Radio Service
GPSD	General Product Safety Directive
GTP	GPRS Tunnel Protocol
HEI	Cloud Service Provider

HR	Human Recruting
ICT	Information and Communication Technology
IETF	Internet Engineering Task Force
IOCTA	Internet Organised Crime Threat Assesment
IoT	Internet of Things
IIoT	Industrial Internet of Things
IP	Internet Protocol
IS	Islamic State
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Internet Technology
ITU	International Telecommunication Unit
KEM	Key Encapsulation Mechanism
KPI	Key Performance Indicator
LDAP	Lightweight Directory Access Protocol
LTE	Long Term Evolution
M	Month
MEC	Mobile Edge Computing
MDR	Medical Device Regulation
ML	Machine Learning
MOOC	Massive Open Online Courses
NBC	National Broadcasting Company
NFV	Network Functions Virtualisation
NIS	Network and Information System
NIST	National Institute of Standards and Technology
OPEX	Operational Expenditure
OS	Operating System
OSS	Operational Support System
OWASP	Open Web Application Security Project
P	Physical
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
PII	Personal Identifying Information
PIMS	Personal Information Management System
PQC	POst Quantum Cryptography
PSD2	Payment Services Directive 2
QKD	Quantum Key Distribution
Q-tech	Quantum Technology
RX	Recommendation X
RFC	Request For Comment
SAF	Security Assurance Framework
SDO	Standard Developing Organization
SDN	Software-Defined Network
SIP	Session IP

SME	Smal and Medium Sized Enterprise
SMS	Short Messaging Service
SOC	Security Operation Center
SOP	State of Play
SOTA	State of the Art
SPDX	Software Package Data Exchange
SQL	Structured Query Language
SS7	Signaling System 7
T	Things
TCB	Trusted Computing Base
TEE	Trusted Execution Environmentt
TG	Threat Group
TLS	Transport Layer Security
TX.Y	Task TX.Y
UAV	Unmanned Aerial Vehicle
US	United States
V	Virtual
VM	Virtual Machine
VOIP	Voice Over IP
VTC	Video Teleconferencing
WP	Work Package
XML	Extended Markup Language
XXE	XML External Entities

References

[1] F. Ambrosio, D. Rückert, and C. Weiss. Who is prepared for the new digital age? - Evidence from the EIB Investment Survey. Technical report, European Investment Bank, Luxembourg, Luxembourg, April 2020, accessed Dec. 18, 2020.

[2] European Parliament Research Service. Digital Sovereignty for Europe. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf, July 2020, accessed Dec. 18, 2020.

[3] European Commission. Rethinking Strategic Autonomy in the Digital Age . https://op.europa.eu/en/publication-detail/-/publication/889dd7b7-0cde-11ea-8c1f-01aa75ed71a1/language-en/format-PDF/source-118064052, July 2019, accessed Dec. 18, 2020.

[4] European Union Agency For Cybersecurity (ENISA). Consultation Paper – EU ICT Industrial Policy: Breaking the Cycle of Failure. https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/eu-ict-industry-consultation-paper/at_download/file, August 2019, accessed Dec. 18, 2020.

[5] intel. A Guide to Internet of Things Infographic. https://www.intel.co.uk/content/www/uk/en/internet-of-things/infographics/guide-to-iot-new.html, accessed Dec. 18, 2020.

[6] O. Garcia-Morchon, S. Kumar, and M. Sethi. Internet of Things (IoT) Security: State of the Art and Challenges. RFC 8576 (Informational), April 2019.

[7] ITU-T - Telecommunication Standardization Sector of ITU. Y.4806: Security Capabilities Supporting Safety of the Internet of Things . Recommendation Y.4806, ITU-T, Geneva, Switzerland, November 2017.

[8] Cyber Security for Consumer Internet of Things: Baseline Requirements. https://tinyurl.com/etsi-baseline-requirement, April 2020, accessed Dec. 24, 2020.

[9] European Union Agency For Cybersecurity (ENISA). Cyber Security and Resilience of Smart Cars . https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars/, Januar 2017, accessed Dec. 18, 2020.

[10] European Union Agency For Cybersecurity (ENISA). Smart Grid Threat Landscape and Good Practice Guide . https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide, December 2013, accessed Dec. 18, 2020.

[11] European Union Agency For Cybersecurity (ENISA). Threat Landscape for Smart Home and Media Convergence. https://www.enisa.europa.eu/publications/threat-landscape-for-smart-home-and-media-convergence, February 2015, accessed Dec. 18, 2020.

[12] European Union Agency For Cybersecurity (ENISA). Threat Landscape and Good Practice Guide for Internet Infrastructure. https://www.enisa.europa.eu/publications/iitl, January 2015, accessed Dec. 18, 2020.

[13] GSMA. Mobile Telecommunications Security Threat Landscape, Final Report. https://www.gsma.com/security/wp-content/uploads/2020/02/2020-SECURITY-THREAT-LANDSCAPE-REPORT-FINAL.pdf, January 2020, accessed Dec. 18, 2020.

[14] European Union Agency For Cybersecurity (ENISA). Cloud Security Guide for SMEs. https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes, April 2015, accessed Dec. 18, 2020.

[15] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert. Practical Attacks Against Privacy and Availability in4G/LTE Mobile Communication Systems. In Network and Distributed System Security Symposium, number 1-15 in NDSS, San Diego, C.A., USA, February 2016.

[16] S.R. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino. LTEInspector: A Systematic Approach forAdversarial Testing of 4G LTE. In Network and Distributed System Security Symposium, number 1-37 in NDSS, San Diego, C.A., USA, February 2018.

[17] M. Chlosta, D. Rupprecht, T. Holz, and C. Pöpper. LTE Security Disabled: Misconfiguration in Commercial Networks. In 12th Conference on Security and Privacy in Wireless and Mobile Networks, WiSec, pages 261–266, New York, N.Y., USA, May 2019. Association for Computing Machinery.

[18] GSMA. Mobile Telecommunications Security Threat Landscape. https://www.gsma.com/security/wp-content/uploads/2020/02/2020-SECURITY-THREAT-LANDSCAPE-REPORT-FINAL.pdf, January 2019, accessed Dec. 18, 2020.

[19] European Union Agency For Cybersecurity (ENISA). Threat Landscape Report 2018 . https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018, January 2019, accessed Dec. 18, 2020.

[20] European Union Agency For Cybersecurity (ENISA). ENISA Study on the Security Aspects of Virtualization. https://www.enisa.europa.eu/news/enisa-news/enisa-study-on-the-security-aspects-of-virtualization, accessed Dec. 18, 2020.

[21] Top Threats to Cloud Computing: Egregious Eleven Deep Dive. https://cloudsecurityalliance.org/artifacts/top-threats-egregious-11-deep-dive/, September 23, 2020, accessed Dec. 24, 2020.

[22] U. von der Leyen. A Union that strives for moreMy agenda for Europe. https://www.europarl.europa.eu/resources/library/media/20190716RES57231/20190716RES57231.pdf, July 2019, accessed Dec. 18, 2020.

[23] Gartner, Inc. What Edge Computing Means for Infrastructure and Operations Leaders. https://tinyurl.com/gartner-edge, October 2018, accessed Dec. 18, 2020.

[24] European Union Agency For Cybersecurity (ENISA). Big Data Threat Landscape. https://www.enisa.europa.eu/publications/bigdata-threat-landscape/, January 2016, accessed Dec. 18, 2020.

[25] OWASP FOundation, Inc. OWASP Top 10 - 2017 The Ten Most Critical Web Application Security Risk. https://tinyurl.com/top10-owasp, 2017, accessed Dec. 18, 2020.

[26] SANS. CWE SANS TOP 25 Most Dangerous Software Errors. https://tinyurl.com/sans-top-25, accessed Dec. 18, 2020.

[27] ISO. ISO/IEC 27001:2013 - Information Technology - Security Techniques - Information Security Management Systems - Requirements. Technical Report ISO/IEC 27001:2013, International Organization for Standardization, Geneva, Switzerland, October 2013, accessed Dec. 18, 2020.

[28] European Union Agency For Cybersecurity (ENISA). Cyber Security Culture in Organisations . https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations, February 2018, accessed Dec. 18, 2020.

[29] R.M. Blank and P.D. Gallagher. Guide for Conducting Risk Assessments. Technical Report NIST Special Publication 800-30, National Institute of Standards and Technology, Gaithersburg, MD, USA, September 2012, accessed Dec. 18, 2020.

[30] Europol, EC3 European Cybercrime Centre. Internet Organised Crime Threat Assessment. https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf, 2018, accessed Dec. 18, 2020.

[31] Europol. A Savety Guide for the ”New Normal” After COVID-19. https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/safety-guide-for-new-normal-after-covid-19, accessed Dec. 18, 2020.

[32] Europol. COVID-19 Sparks Upward Trend in Cybercrime. https://www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime, October 2020, accessed Dec. 18, 2020.

[33] KPMG. Staying on Top of Changing Crime Patterns. https://home.kpmg/xx/en/home/insights/2020/05/staying-on-top-of-changing-crime-patterns.html, accessed Dec. 18, 2020.

[34] European Union Agency For Cybersecurity (ENISA). Understanding and Dealing with Phishing During the COVID-19 Pandemic . https://tinyurl.com/enisa-dealing-phishing, May 6, 2018, accessed Dec. 18, 2020.

[35] Deloitte. COVID-19's Impact on Cybersecurity. https://www2.deloitte.com/ng/en/pages/risk/articles/covid-19-impact-cybersecurity.html, accessed Dec. 18, 2020.

[36] KPMG. Key Cyber Risks for Banks during COVID-19. https://home.kpmg/xx/en/home/insights/2020/05/key-cyber-risks-for-banks-during-covid-19.html, accessed Dec. 18, 2020.

[37] KPMG. The Rise of Ransomware Ruring COVID-19. https://home.kpmg/xx/en/home/insights/2020/05/rise-of-ransomware-during-covid-19.html, accessed Dec. 18, 2020.

[38] Panda Security. COVID-19 Cybersecurity Statistics. https://www.pandasecurity.com/en/mediacenter/news/covid-cybersecurity-statistics/, accessed Dec. 18, 2020.

[39] European Union Agency For Cybersecurity (ENISA). Cybersecurity in the Healthcare Sector During COVID-19 Pandemic . https://tinyurl.com/enisa-dealing-phishing-healthc, May 2020, accessed Dec. 18, 2020.

[40] McKinsey & Company. COVID-19 Crisis Shifts Cybersecurity Priorities and Budgets. https://tinyurl.com/mckinsey-risk-budget, accessed Dec. 18, 2020.

[41] PWC. Managing the Impact of COVID-19 on Cyber Security. https://www.pwccn.com/en/issues/cybersecurity-and-data-privacy/covid-19-impact-mar2020.pdf, March 2020, accessed Dec. 18, 2020.

[42] J. Gao, P. Zheng, Y. Jia, H. Chen, Y. Mao, S. Chen, Y. Wang, H. Fu, and J. Dai. Mental Health Problems and Social Media Exposure During COVID-19 Outbreak. PLOS ONE, pages 1–10, April 2020.

[43] Y. Huang and N. Zhao. Generalized Anxiety Disorder, Depressive Symptoms and Sleep Quality During COVID-19 Outbreak in China: A Web-based Cross-sectional Survey. Psychiatry Research, June 2020.

[44] Europol. COVID-19 Shopping Scams. https://www.europol.europa.eu/covid-19/covid-19-shopping-scams, accessed Dec. 18, 2020.

[45] Europol. Staying Safe During COV¿ID-19: What You Need to Know. https://www.europol.europa.eu/activities-services/staying-safe-during-covid-19-what-you-need-to-know, November 12 2020, accessed Dec. 18, 2020.

[46] European Commission. Scams Related to COVID-19. https://ec.europa.eu/info/departments/justice-and-consumers/justice-and-consumers-funding-tenders/funding-areas/consumer-programme-cp/enforcement-consumer-protection/scams-related-covid-19_en, April 2020, accessed Dec. 18, 2020.

[47] European Commission. Europe: The Keys To Sovereignty. https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-keys-sovereignty_en, September 11, 2020, accessed Dec. 18, 2020.

[48] European Processor Initiative. First Steps Towards a Made-in-Europe High-Performance Microprocessor. https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-keys-sovereignty_en, June 4, 2019, accessed Dec. 18, 2020.

[49] European Commission. Quantum Technologies Flagship. https://ec.europa.eu/digital-single-market/en/quantum-technologies-flagship, accessed Dec. 18, 2020.

[50] Federal Ministry for Economic Affairs and Energy. GAIA-X: A Federated Data Infrastructure for Europe. https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html, accessed Dec. 18, 2020.

[51] Federal Ministry for Economic Affairs and Energy. A Responsible Internet: Increasing Trust in the Foundation of Digital Societies. https://tinyurl.com/sidnlabs-report, November 5, 2020, accessed Dec. 18, 2020.

[52] Investopedia. 10 Biggest Telecommunications Companies. https://www.investopedia.com/articles/markets/030216/worlds-top-10-telecommunications-companies.asp, November 17, 2020, accessed Dec. 18, 2020.

[53] GSMA. Network Equipment Security Assurance Scheme (NESAS). https://www.gsma.com/security/network-equipment-security-assurance-scheme/, accessed Dec. 18, 2020.

[54] Pope, M. Security Assurance Methodology (SCAS) for 3GPP Network Products. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2345, September 2020, accessed Dec. 18, 2020.

[55] Federal Ministry for Economic Affairs and Energy. A Taxonomy and Terminology of Adversarial Machine Learning. https://csrc.nist.gov/publications/detail/nistir/8269/draft, October, 2019, accessed Dec. 18, 2020.

[56] F. Cavaliere, J. Mattsson, and B. Smeets. The Security Implications of Quantum Cryptography and Quantum Computing. Network Security, 2020(9):9 – 15, September 2020.

[57] U.S. Department of Energy. U.S. Department of Energy Unveils Blueprint for the Quantum Internet at ‘Launch to the Future: Quantum Internet’ Event. https://tinyurl.com/energy-gov-report, July 23, 2020, accessed Dec. 18, 2020.

[58] CONCORDIA Consortium. Assessing the courses for Cybersecurity professionals already developed by CONCORDIA partners. https://www.concordia-h2020.eu/wp-content/uploads/2020/04/CONCORDIA-AssessmentOfCoursesT3.4-ForWebsite.pdf, December 2019, accessed Dec. 18, 2020.

[59] OECD. Transformative Technologies and Jobs of the Future. http://www.oecd.org/science/inno/transformative-technologies-and-jobs-of-the-future.pdf, March 2018, accessed Dec. 23, 2020.

[60] T. Scholtz. Rethink the Security and Risk Strategy. https://emtemp.gcom.cloud/ngw/globalassets/en/publications/documents/rethink-security-risk-strategy-ebook.pdf, accessed Dec. 18, 2020.

[61] TÜV Rheinland. Cyber Security Trends 2019. https://insights.tuv.com/cyber-security-trends-2019-whitepaper, accessed Dec. 18, 2020.

[62] VentureBeat. Why cybersecurity workers are some of the hardest to retain. https://tinyurl.com/venturebeat-1, November 11, 2017, accessed Dec. 18, 2020.

[63] European Cyber Security Organisation. Position Paper - Gaps in European Cyber Education and Professional Training. https://ecs-org.eu/documents/publications/5fdb282a4dcbd.pdf, November 2017, accessed Dec. 18, 2020.

[64] M. van Zadelhoff. Cybersecurity Has a Serious Talent Shortage. Here's How to Fix It. https://tinyurl.com/harvard-business-report, May 4, 2017, accessed Dec. 18, 2020.

[65] World Economic Forum. Jobs of Tomorrow - Mapping Opportunity in the New Economy. http://www3.weforum.org/docs/WEF_Jobs_of_Tomorrow_2020.pdf, January 2020, accessed Dec. 18, 2020.

[66] European Commission. Upskilling for Life After the Pandemic: Commission Launches New Digital Competence Guidelines. https://tinyurl.com/ec-upskilling-life, July 13, 2020, accessed Dec. 18, 2020.

[67] European Commission. Skills for SMEs – Cybersecurity, Internet of Things and Big Data for Small and Medium-Sized Enterprises. https://op.europa.eu/en/publication-detail/-/publication/82aa7f66-67fd-11ea-b735-01aa75ed71a1/language-en, December 2019, accessed Dec. 18, 2020.

[68] T. Moore. The Economics of Cybersecurity: Principles and Policy Options. International Journal of Critical Infrastructure Protection, 3(3):103–117, December 2010.

[69] Afcea Cyber Committee. The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment. International Journal of Critical Infrastructure Protection, pages 1–15, October 2013.

[70] G. Locke and P.D. Gallagher. Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Technical Report NIST Special Publication 800-37 Revision 1, National Institute of Standards and Technology, Gaithersburg, MD, USA, December 2019, accessed Dec. 18, 2020.

[71] Information Technology Laboratory. Security and Privacy Controls for Federal Information Systems and Organizations. https://nvd.nist.gov/800-53, accessed Dec. 18, 2020.

[72] Microsoft. The Threats to Our Products. https://www.microsoft.com/security/blog/2009/08/27/the-threats-to-our-products/, August 2009, accessed Dec. 18, 2020.

[73] K.W. Preneel, R. Scandariato, W. Joosen, and M. Deng. LINDDUN: A Privacy Threat Analysis Framework. Computers & Security, pages 1–23, February 2020.

[74] A. Shostack. Experiences Threat Modeling at Microsoft. In International Conference on Model Driven Engineering Languages and Systems, Workshop on Modeling Security, volume 413, pages 1–11, Toulouse, France, January 2008. CEUR-WS.org.

[75] E. Rich, J.J. Gonzalez, Y. Qian, F.O. Sveen, J. Radianti, and S. Hillen. Emergent Vulnerabilities in Integrated Operations: A Proactive Simulation Study of Economic Risk. International Journal of Critical Infrastructure Protection, 2(3):110 – 123, October 2009.

[76] B. Rodrigues, M. Franco, G. Parangi, and B. Stiller. SEConomy: A Framework for the Economic Assessment of Cybersecurity. In 16th International Conference on Economics of Grids, Clouds, Systems, and Services, GECON, pages 154–166, Basel, Switzerland, September 2019. Springer International Publishing.

[77] M.F. Franco, B. Rodrigues, and S. Stiller. MENTOR: The Design and Evaluation of a Protection Services Recommender System. In 15th International Conference on Network and Service Management, CNSM, pages 1–7, New York, NY, USA, October 2019. IEEE.

[78] Potomac Institute for Policy Studies. Cyber Readiness Index Country Profiles. https://www.potomacinstitute.org/academic-centers/cyber-readiness-index, accessed Dec. 18, 2020.

[79] European Commission. Europe's Moment: Repair and Prepare for the Next Generation. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_940, May 27, 2020, accessed Dec. 18, 2020.

[80] European Court of Auditors. Challenges to Effective EU Cybersecurity Policy. https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf, March 2019, accessed Dec. 18, 2020.

[81] European Union Agency For Cybersecurity (ENISA). National Cyber Security Strategy . https://resilience.enisa.europa.eu/enisas-ncss-project, accessed Dec. 18, 2020.

[82] CONCORDIA Consortium. Deliverable D4.1: 1st Year Report on Cybersecurity Threats. https://www.concordia-h2020.eu/wp-content/uploads/2020/06/D4.1_Ready_for_Submission_D4.1-final_revised.pdf, April 2020, accessed Dec. 18, 2020.

[83] European Union Law. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation COM/2020/264 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264, June 2020, accessed Dec. 18, 2020.

[84] European Commission. Cybersecurity – Review of EU Rules on the Security of Network and Information Systems . https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Revision-of-the-NIS-Directive, June 2020, accessed Dec. 18, 2020.

[85] European Commission. Combined Evaluation Roadmap/Inception Impact Assessment, Revision of the NIS Directive. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=PI_COM:Ares(2020)3320999&from=EN, 2020, accessed Dec. 18, 2020.

[86] European Union Law. Report from the commission to the european parliament and the council assessing the consistency of the approaches taken by member states in the

identification of operators of essential services in accordance with article 23(1) of directive 2016/1148/eu on security of network and information systems com/2019/546 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0546, October 2019, accessed Dec. 18, 2020.

[87] European Commission. Cybersecurity: Commission urges Belgium, Hungary and Romania to Comply With Their Obligations Regarding Operators of Essential Services. https://tinyurl.com/ec-digmarket-hungary-romania, October 30, 2020, accessed Dec. 18, 2020.

[88] European Commission. Proposal for a Regulation on European Data Governance (Data Governance Act). https://tinyurl.com/ec-digmarket-reg-proposal, November 25, 2020, accessed Dec. 18, 2020.

[89] I. Nai Fovino, R. Neisse, A. Lazari, G.-L. Ruzzante, N. Polemi, and M. Figwer. European Cybersecurity Centres of Expertise Map - Definitions and Taxonomy. Technical Report EUR 29332 EN OPOCE KJ-NA-29332-EN-N, European Commission, Brussels, Belgium, 2020, accessed Dec. 18, 2020.

[90] European Union Agency For Cybersecurity (ENISA). Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. https://tinyurl.com/enisa-behavioural-aspects, April 2019, accessed Dec. 18, 2020.

[91] ISO. ISO in brief - Great Things Happen When the World Agrees. https://www.iso.org/standard/54534.html, August 2019, accessed Dec. 18, 2020.

[92] Z. Xie, J. Hall, I.P. McCarthy, M. Skitmore, and L. Shen. Standardization Efforts: The Relationship Between Knowledge Dimensions, Search Processes and Innovation Outcomes. Technovation, 48-49:69–78, February-March 2016.

[93] I. Nai Fovino, R. Neisse, J.L. Hernandet-Ramos, N. Polemi, G.-L. Ruzzante, M. Figwer, and A. Lazari. A Proposal for a European Cybersecurity Taxonomy. Technical Report JRC118089, European Commission, Brussels, Belgium, 2019, accessed Dec. 18, 2020.

[94] M. Mlkva, V. Prajova, B. Yakimovich, A. Korshunov, and I. Tyurin. Standardization - One of the Tools of Continuous Improvement. In International Conference on Manufacturing Engineering and Materials, volume 149, pages 329–332, Novy Smokovec, Slovakia, June 2016. Procedia Engineering.

[95] N. Abdelkafi. Understanding ICT Standardization: Principles and Practice. Number 3748247427. ETSI, Sophia Antipolis, Frankreich, May 2019.

[96] K. Rantos, A. spyros, A. Papanikolaous, A. Kritsa, C. Illoudis, and V. Katos. Interoperability Challenges in the Cybersecurity Information Sharing Ecosystem . Computers, 9(1):1–17, February 2020.

[97] M. Elkhodr, S. Shahrestani, and H. Cheung. The Internet of Things: New Interoperability, Management and Security Challenges. ArXiv, abs/1604.04824, 2016.

[98] European Union Law. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance), PE/86/2018/REV/1. https://eur-lex.europa.eu/eli/reg/2019/881/oj, April 2019, accessed Dec. 18, 2020.

[99] European Union Agency For Cybersecurity (ENISA). Cybersecurity Certification: EUCC Candidate Scheme. https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme, July 2020, accessed Dec. 18, 2020.

[100] European Union Agency For Cybersecurity (ENISA). After cloud...cybersecurity certification: launching the ENISA ad hoc Working Group on Cloud Services . https://tinyurl.com/enisa-after-cloud, March 6, 2020, accessed Dec. 18, 2020.

[101] European Parliament Legislative Observatory. European Cybersecurity Industrial, Technology and Research Competence Centre and Network of National Coordination Centres - 2018/0328(COD). https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2018/0328(COD)&l=en, 2018, accessed Dec. 18, 2020.

[102] European Union Law. COM (2018) 630: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018. https://eur-lex.europa.eu/procedure/EN/2018_328, 2018, accessed Dec. 18, 2020.

[103] European Commission. REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-centres-regulation-630_en.pdf, September 2018, accessed Dec. 18, 2020.

[104] European Commission. COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT. https://ec.europa.eu/transparency/regdoc/rep/10102/2018/EN/SWD-2018-403-F1-EN-MAIN-PART-1.PDF, September 2018, accessed Dec. 18, 2020.