CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

Work Package 4: Supplement to Deliverable D4.4:

# Cybersecurity Roadmap for Europe

**Abstract:**
This document provides summary takeaways across the dimensions of the CONCORDIA's Cybersecurity Roadmap for Europe detailed in D4.4.

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 | *N/A - Supplemental Document* |
| Actual date of delivery | *31.12.2022* |
| Deliverable dissemination level | *Public* |
| Editors | *Gabi Dreo (UniBW/CODE)*<br>*Corinna Schmitt (UniBW/CODE)*<br>*Arthur van der Wees (Arthur's Legal)*<br>*Neeraj Suri (ULANC)* |
| Contributors | *Neeraj Suri (ULANC)*<br>*Luis Barriga (Ericsson)*<br>*Muriel Franco (UZH)*<br>*Burkhard Stiller (UZH)*<br>*Felicia Cutas (EIT DIGITAL)*<br>*Kostas Lampropoulos (UP)*<br>*Claudio Ardagna (UMIL)*<br>*Arthur Van der Wees (ARTHUR'S LEGAL)*<br>*Dimitra Stefanatou (ARTHUR'S LEGAL)*<br>*Prakriti Pathania (ARTHUR'S LEGAL)*<br>*Argyro Chatzopoulous (TUV TRUST)*<br>*Gabi Dreo (UniBW/CODE)*<br>*Aiko Pras (UT)*<br>*Michael Sirivianos (CUT)*<br>*Jean-Yves Marion (UL)*<br>*Cristian Hesselman (SIDN)* |
| Quality assurance | *Tatjana Welzer (Univ of Maribor)*<br>*Lili Nemec Zlatolas (Univ of Maribor)*<br>*Paolo de Lutiis (Telecom Italia)*<br>*Remco Poortinga – van Wijnen (SurfNet)*<br>*Boning Feng (Oslo Metropolitan Univ)* |

# 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 |

| | | |
|---|---|---|
| TÜ V TRUST IT | TUV TRUST IT GmbH | Germany |
| TI | Telecom Italia SPA | Italy |
| Efacec | EFACEC Electric Mobility SA<br>(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~~ |
| NCSA | Ministry of Digital Governance – National Cyber Security Authority | 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 |
| FER | University of Zagreb, Faculty of Electrical Engineering and Computing | Croatia |
| ICENT | Innovation Centre Nikola Tesla | Croatia |
| Utilis | Utilis d.o.o | Croatia |
| Polito | Politechnico di Torino | Italy |

# Revisions

| Ver. | Date | By | Overview |
|---|---|---|---|
| *0.1* | *28.08.2022* | *Neeraj Suri (ULANC), Arthur van der Wees (Arthurs Legal)* | *Initial Compilation* |
| *0.5* | *27.09.2022* | *All D4.4 chapter leads* | *Dimension Inputs* |
| *0.9* | *15.10.2022* | *Neeraj Suri (ULANC)* | *Integration* |
| *0.95* | *27.10.2022* | *All D4.4 chapter leads* | *Revisions* |
| *0.96* | *7.11.2022* | *Neeraj Suri (ULANC)* | *Review & Integration* |
| *0.97* | *29.11.2022* | *Neeraj Suri (ULANC)* | *Revision 1 Integration* |
| *0.98* | *7.12.2022* | *Neeraj Suri (ULANC)* | *Revision 2 Integration* |
| *1.0* | *9.12.2022* | *Neeraj Suri (ULANC)* | *Release* |

# Executive Summary

Future global market-dominant products and services will likely 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.

With this context, deliverable D4.4 provides the following:

- Development of a holistic approach on the definition and scope of the Cybersecurity Roadmap for Europe by taking an end-to-end data centric view on security considered over the complete systems chain.
- The identification of the six holistic 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 to keep in mind the 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).
- Prioritizing the recommendations of the roadmaps on the time scale from short-term (next 2-3 years), mid-term (>2025), and long-term (>2030).
- Incorporating summarized feedback from the security community over:
  - Discussions with the pilots CyberSec4Europe, ECHO and SPARTA, alongside ECSO and the EC JRC Atlas team to develop a consolidated inter-pilot view on Cybersecurity considerations and priorities.
  - Discussions with the broader Cybersecurity stakeholder community to recognize their priorities across the CONCORDIA recommendations.

With the full roadmapping details provided in deliverable D4.4, the current document provides 1-page summary snapshots of each of the dimensions covered in the roadmap.

# Contents

# Introduction

Deliverable D4.4 addresses the outcome of task T4.4, which is devoted to the specification of a 'Cybersecurity Roadmap for Europe by CONCORDIA'.

As 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 2022.

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 the following six dimensions (Figure 1) to project a holistic view of European digital sovereignty.

- **Research and Innovation**
- **Education and Skills**
- **Economics and Investments**
- **Legal and Policy**
- **Certification and Standardization**
- **Community Building**

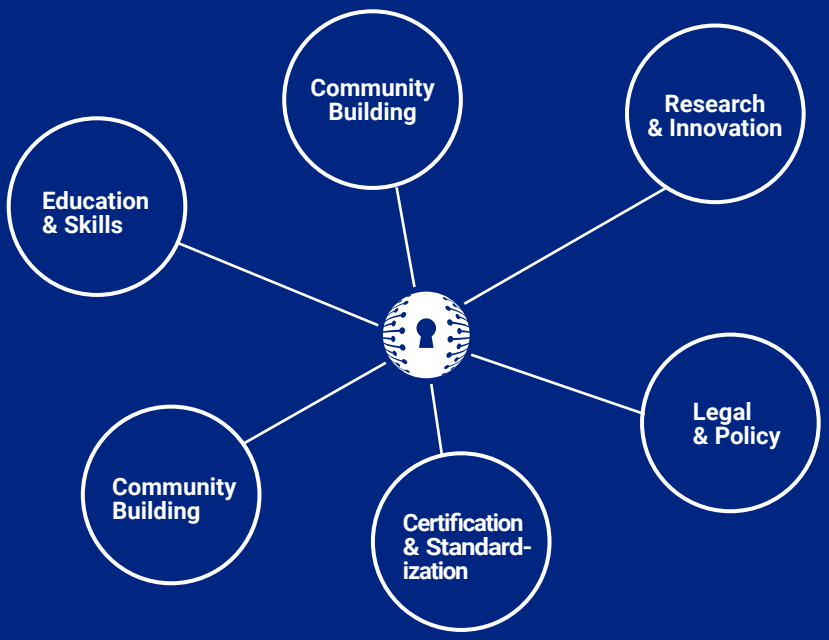
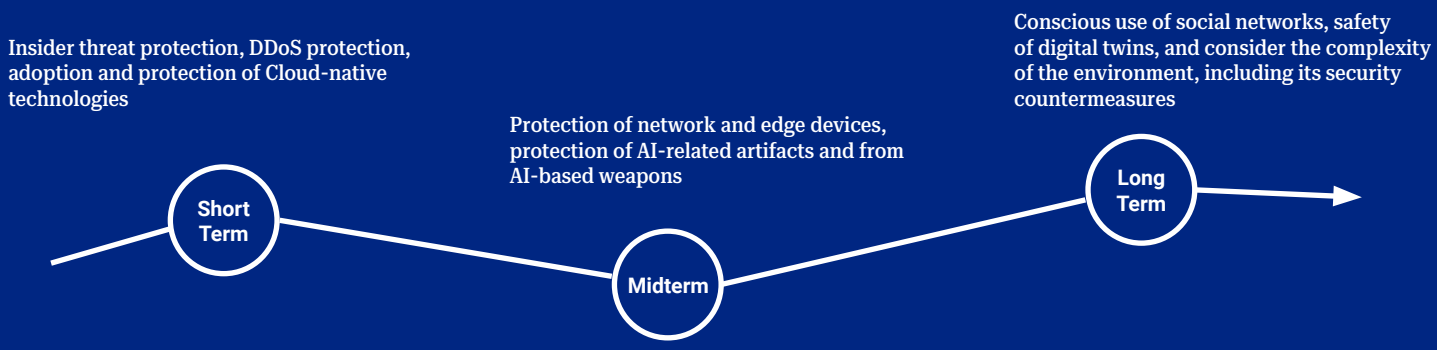



*Figure 1: The CONCORDIA dimensions*

**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 current document captures summary takeaways for each of the dimensions starting with an analysis of the threat landscape. For fuller details, the reader is referred to deliverable D4.4.

# Threat Landscape




The ICT landscape has been revolutionized in the last decade by the introduction of cloud and edge computing, new networking technologies, and artificial intelligence, to name some of the main disruptive innovations. At the same time, it is increasingly challenging for organizations to secure their systems, since traditional protection measures based on perimetral security have proven to be inadequate. The shift to remote work forced by the Pandemic enlarged the IT perimeter to workers' personal devices, and malicious threat actors quickly took advantage of this, exploiting social engineering and the software supply chain to mount attacks. It comes with no surprise that human factor and software supply chain are the most challenging aspects to manage from a security point of view. To make things worse, organizations still suffer from long-standing issues, such as the lack of skills.

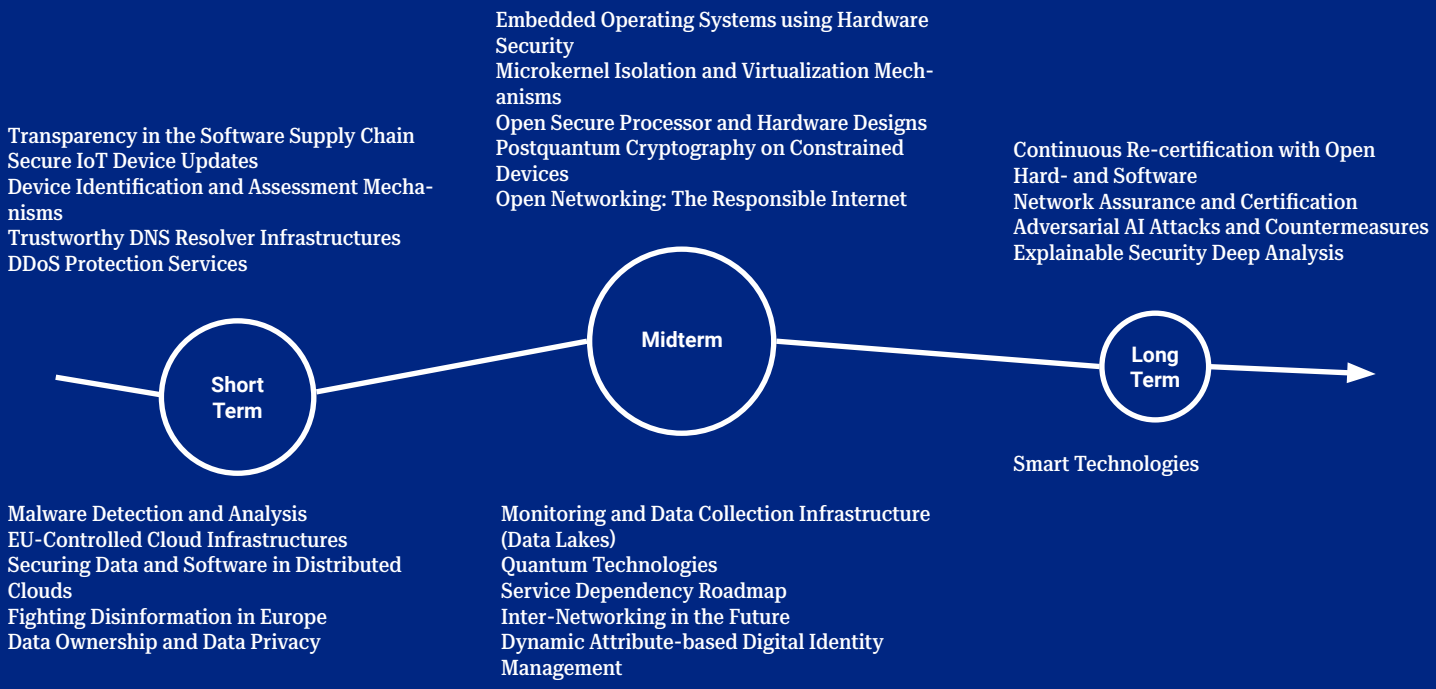
The CONCORDIA threat landscape provides a fine-grained mapping between assets, threats, gaps, countermeasures, and research actions, according to 6 domains: device/IoT (focused on modern systems based on IoT and edge devices), network (focused on interconnections providing data transport), system (focused on cloud and virtualized systems, including operating systems), data (focused on the management and protection of data at all layers of system, including Big Data), application (focused on software and programs, including dependency management, supply chain, services and their life cycle management), and user (focused on issues pertaining users, such as privacy, social networks, and identity management).

One of the most important challenges sits at the confluence of artificial intelligence (AI) and network perimeter-less security. Zero-trust security is a novel security management paradigm, more suited to the modern scenarios characterized by a high mobility of users, where the notion of security perimeter is no longer relevant. In zero-trust security, devices, applications, and users, are untrusted by default, and they have to always and continuously be authenticated, authorized, and validated. AI plays a pivotal role in zero-trust

security, for instance, in continuous user authentication. However, the practical implications and operational challenges remain to be fully understood. It is in fact well-known that AI brings new threats by itself, since AI models can be attacked in peculiar ways (such as model poisoning and model inference). Furthermore, AI models can be a source of threats themselves. Notoriously, an AI model trained on a biased dataset may introduce discrimination and violate the law. It is therefore fundamental to be (at least) aware of the novel challenges posed.

A proper recommendation roadmap must consider short and long-term goals. First, organizations should consider the long-standing issues and consciously move to cloud-native technologies. In the end, organizations should account for AI and its interplay with users and the environment. The summary of recommendations considering the threat landscape are shown herein, with the details available in deliverable D4.4.

# Roadmap for Research and Innovation




The research and innovation roadmap targets three pillars of digital sovereignty of Europe, namely that Europe should have the means to design and manufacture current and future computers, the European citizens should be able to trust that their data will be stored on cloud servers operating under EU legislation, and that Europe provides secure connectivity where data will be exchanged over a responsible Internet. The roadmap describes a total of 25 research and innovation challenges.

Key innovation challenges related to device security are trustworthy hardware and firmware as well as assessment techniques that can verify the authenticity and integrity of devices. Embedded device security mechanisms play a special role given the importance of embedded systems in the industrial sector. Network security research challenges center around the concept of a responsible Internet as well as novel attack prevention schemes and the collection of monitoring data in so-called data lakes.

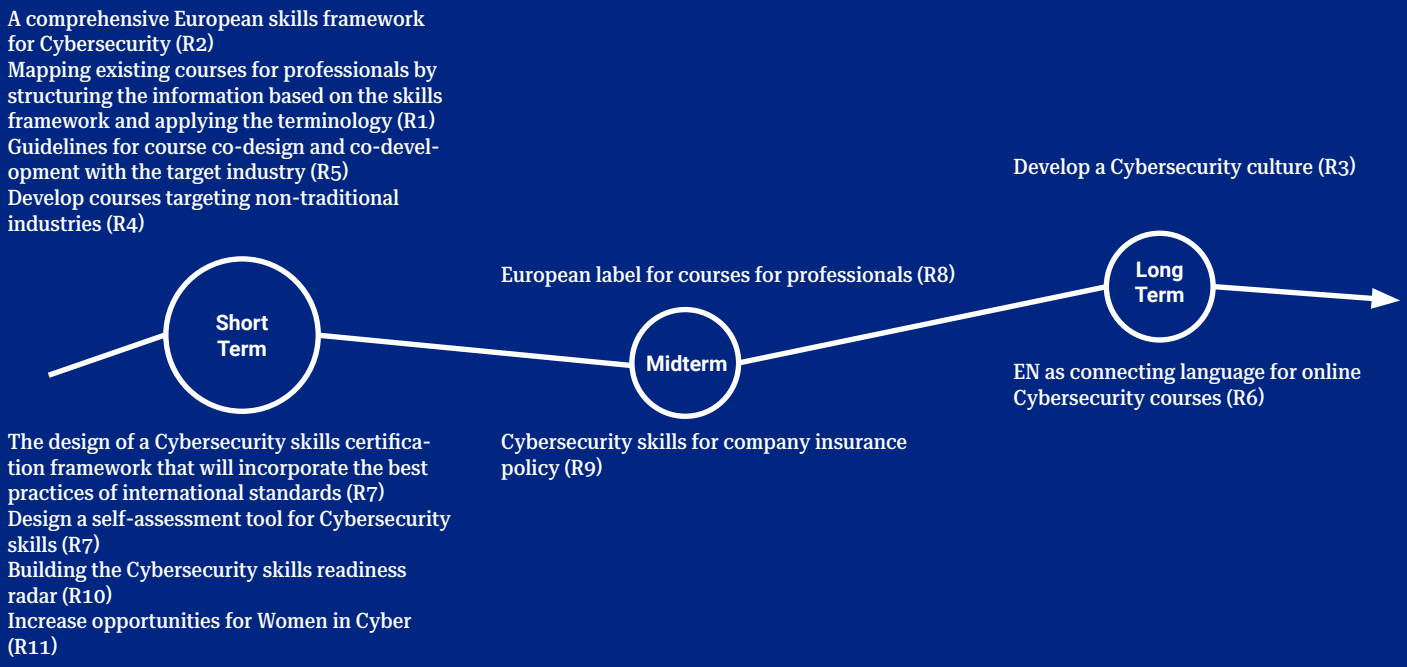
The research challenges identified for software and system security address quantum technologies as well as attacks on artificial intelligence systems

and counter measures and explainable security services. More traditional topics like malware detection and analysis and service dependency analysis will remain relevant. In the context of data and application security, the development of European secure cloud infrastructure is of direct importance. The same holds for the development of techniques that can secure data and software in distributed computing environments. The security aspects of inter-networked smart technologies pose a more longer-term research challenge.

Finally, at the user security level, fighting disinformation in Europe is a key short-term challenge as well as the protection of data ownership and data privacy. The development of decentralized identifiers is a more medium-term innovation challenge.

The summary recommendations are illustrated herein with the details available in deliverable D4.4.

# Roadmap for Education and Skills for Cybersecurity Professionals




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 10 challenges mentioned in the Education chapter of the roadmap are based on our findings when assessing CONCORDIA's courses for cybersecurity professionals' portfolio, on the desk research performed, and the input collected from the stakeholders. They span between the challenges brought by the skills gap, which is still persisting, and the challenges generated by the difficulty of understanding and seeing the training big picture, to issues generated by the heterogeneity of competencies related terminology, lack of a cybersecurity culture and the industry gender biased aspect. In view of addressing these challenges, we are proposing a set of 12 recommendations to be implemented on short/medium/long term.

For each of the recommendation we suggest under "Who" the main actor(s) we consider should lead the implementation, and under "Relevance" the actor(s) impacted/benefiting from the implementation of the recommendation. The recommendations are straight forward and point towards, between others, the needs of mapping the existing offer of trainings in a structured way by applying an agreed terminology, improving the cyber-aware attitude at all levels, building and delivering courses and trainings those content is built on specific needs of the companies while including soft skills and aspects linked to the economics of cybersecurity.

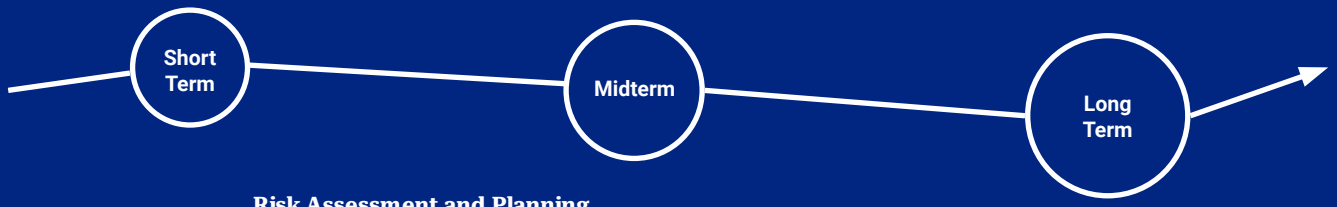
Other recommendations suggest considering the human factor in cybersecurity insurance, increase the opportunities for women in cyber and last but not least, establish an agile governance model for the European education ecosystem.

# Roadmap for Economics

**Training and Education**
Human factor is the major factor making business vulnerable. People with different responsibilities 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.

**Efficient strategies and wide adoption of Cybersecurity for all business in key sectors**
The evolving of approaches to understand risks and guide better investments in Cybersecurity should converge, together with proper regulations, for the promotion of Cybersecurity as part of every business strategy.




**Risk Assessment and Planning**
Understanding 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.

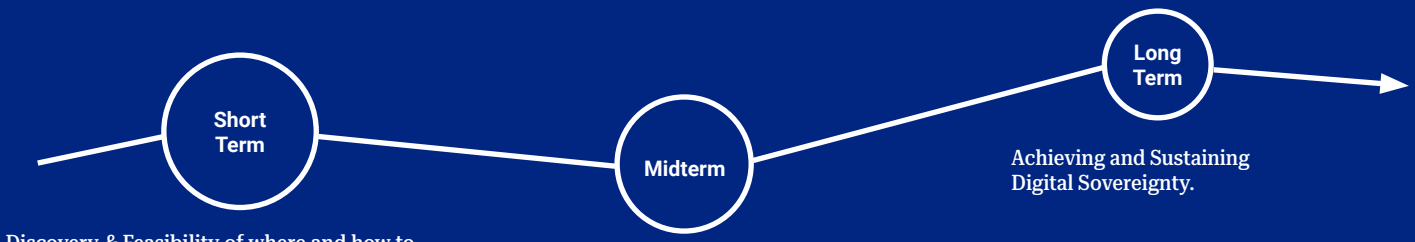
The economics of cybersecurity started more recently to become a major pillar for the operations and costs associated with cybersecurity-related investments. While the demand to provide even stronger security measures to IT system already deployed in society is very visible in today's society, their dedicated importance does clearly vary. 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.

Due to very high degree of interactions, embedding, and cooperation of IT systems, 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. 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

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. Therefore, main economic incentives also have to be considered to support suitable and privacy-preserving information-sharing regarding potential and experienced threats to create a strong community. Also, it is important to see the changing of cybersecurity culture as a long-term goal, thus, moving beyond the short-term training and education for cybersecurity awareness. The summary of recommendations considering cybersecurity economics are shown herein, with the details available in deliverable D4.4.

# Roadmap for Investments




Discovery & Feasibility of where and how to effectively build Digital Sovereignty, start building those components, and preparing to start building other components.

Building and initial achievement of Digital Sovereignty.

Achieving and Sustaining Digital Sovereignty.

In order to enhance cybersecurity in the EU, strategic investments in the right infrastructure, people, resources, skills, financial instruments and structures to build, achieve and sustain cybersecurity is essential. The chapter regarding investments in cybersecurity dives into how existing cybersecurity knowledge, competences and capabilities can be further built upon, double looped to identify gaps and vulnerabilities which can then be improved and further amplified to fortify cybersecurity capabilities in the EU. It also aims at creating a framework for identifying value propositions, business models, financial models which can be used by organizations, sectors, member states and the EU and continuously improved in line with evolving market trends. It also sheds light on other challenges and scenarios that can be looked into from an investment perspective.

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 the Cybersecurity Roadmap for Europe by CONCORDIA. These requires substantial investments in resources, both in people, knowledge, competencies, skills and funds, as well in all sorts of hybrid technical, organisational and economical infrastructures.

There is a profound investment gap between the EU and other parts of the world, due to the fragmented and disorganized public and private investments across the Europe. This, for instance, leaves no choice for European cybersecurity ventures but to seek financial support and market opportunities from non-European organisation with all costs including losing the control over their companies.

The solution is to facilitate investments in the right infrastructure, people, resources, skills, competencies, financial instruments in order to equip the

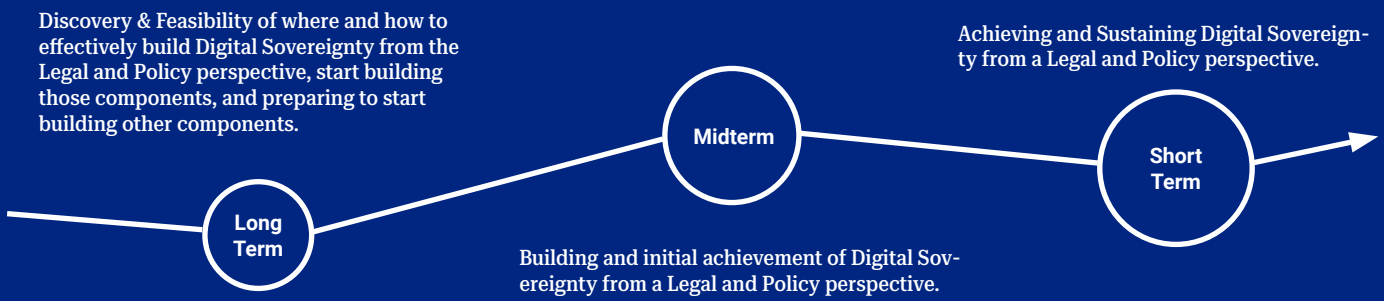
European organisations with the right cybersecurity capabilities that the European internal market as well as markets outside of the EU are willing to pay for, and thus, they can grow, scale and succeed as true European champions in cybersecurity sectors.

However, development of such investments strategies requires proper value propositions with a dynamic and multi-dimensional perspective. This will lead to the development of business models that generate return on investment in line with the appreciated or sought-after values and interest of the various investor including but not limited to monetary returns, individual and societal values.

For example, the holistic consideration of return of investment provides the potential investor with a viable and sustainable ecosystem where the various returns can cater to and amplify each other. Once the value sensitive business models are in place, the next step is mapping and plotting the various investment opportunities, sectors and capabilities. For instance, there are many research innovation actions and respectively innovation action projects in the cybersecurity domain, (co)funded under the various EU Funding Programmes, past and present, which outcomes are ready to be orchestrated, marketed and implemented, at local, regional, national and EU-scale.

The summary recommendations are illustrated herein with the details available in D4. 4.

# 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.

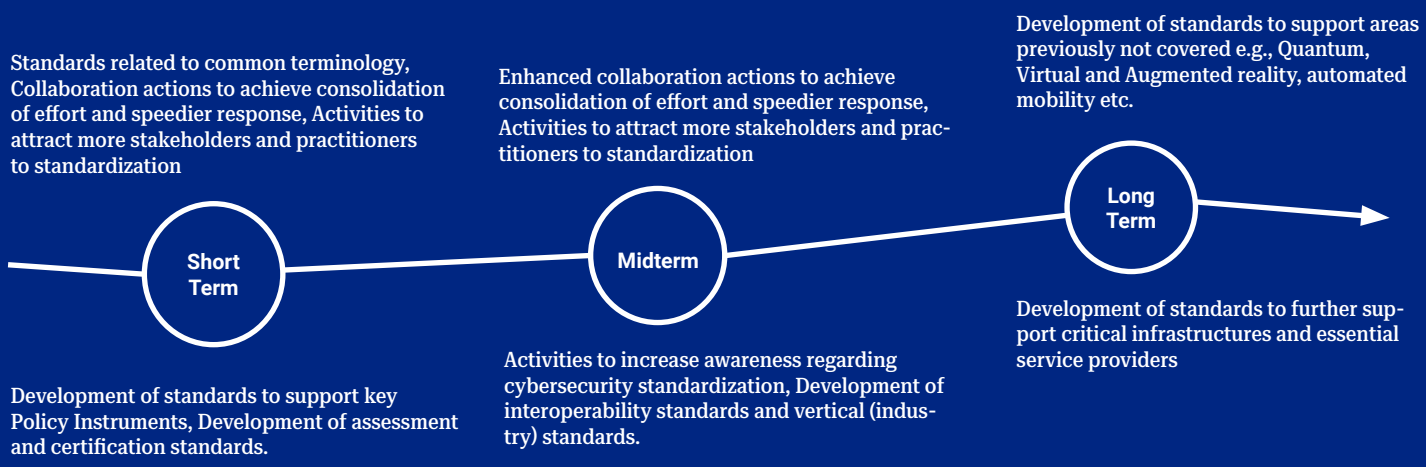
This leads to many and various challenges to address, risks to mitigate, impact to avoid, re-organise or otherwise coordinate and orchestrate detrimental consequences and related responsibility, accountability, liability, and enforcement capabilities, as well as renewed or otherwise improved monitoring 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. The Legal & Policy roadmap recommendations and related mini-roadmaps addresses these and other challenges, for the short, mid and long term.

One of the challenges regard the need to create a Trusted Experience Sharing framework, which would allow European cybersecurity players to share a great wealth of knowledge, experience, lesson learned, best practices. Furthermore, there is a need of mapping EU cybersecurity products, systems and services in an expanding and hyperconnected the cybersecurity domain. To map the existing capacity, both in terms of specific domains and compe-

tencies, and highlight similarities, synergies and complementarities in the European space. There is also a need for a more uniform implementation of cybersecurity standards and regulations across the Union. It is important that all European member states adopt and implement the same level of sector-coverage as the other member states, or at least to a certain minimum yet sufficient level. This also puts on the radar the need for better coordination for pre-procurement of cybersecurity EU products, systems and services. It is recommended that a methodology, as well as a common reference model, that also includes elements regarding data management, performance and negotiation capabilities is established.

The summary recommendations are illustrated herein with fuller details available in D4.4.

# Roadmap for Standardisation & Certification




Standards can contain terms and definitions, can provide guidelines and best practices and provide directions and requirements. Standards contain information collected from a variety of sources and (ideally) through the collaboration and consensus of a number of knowledgeable interested parties.

Cybersecurity standardisation is facing challenges like the low awareness of interested parties regarding standards and the standardisation processes, the relevant latency in the development of standards, the lack of common terminology, the lack of recognition and adoption of the standards, which in turn leads to the implementation of standards by different entities that cover the same domain and the complete lack of standards in other domains etc.


https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

In the roadmap deliverable D4.4, 55 activities have been identified which could help with overcoming the challenges of cybersecurity standardisation. These activities have been split into short term, midterm and long term and represented herewith with an associated timeline.

Certification is the third-party attestation related to products, processes, systems or persons. Certification can apply to a product, process, system, person or body.

To support the aims of current and future policy instruments, recognized, value enhancing, safe and secure certification schemes should exist. Currently, certification faces many challenges with the most prominent ones being: lack of common recognized certification schemes for ICT products, services and processes, existence of certification schemes that cover the same subject with a scope depending on the country, the region, the national legislation or the private or public organization that has developed them, the lack of common standards on which to build certification schemes and the lack of methods and tools to facilitate agile, secure and privacy preserving certification.

In the roadmap deliverable D4.4, 44 activities are identified which could help with overcoming the challenges of cybersecurity certification. These activities have been split into short term, midterm and long term and represented herewith with a recommended timeline. The details are provided in the deliverable D4.4.

# Roadmap for Community Building


If you want to go fast, go alone. If you want to go far, go together' is a famous universal wisdom. It is also basically embraced by and embedded in the Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (2021/887). 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.

It becomes evident that the regulation aims to create collaboration in four (4) domains; (i) Sovereignty & Collaborative Resilience, (ii) Economic Development & Competition, (iii) Research & Innovation, and (iv) Education, Skills & Jobs, which are intertwined as one affects the other – positively respectively negatively, in the short, mid or long term. –, as one requires the other, and as one adds to and augments the other.

The community building chapter defines strategies 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.

Getting to know ourselves is the first step for the community building which leads to building trust, and thereafter add further trust layers on top of that. Community building is a major challenge for European cybersecurity, as without teamwork one would miss out on a prerequisite success factor. Therefore, for a strong community the relevant stakeholders' needs and expectations, from all perspectives, and in the various phases need to be identified and in the mid-term the creation of living labs and local, regional, national and (European) sectorial competence centres to attract diverse ideas and perspectives to relevant challenges should be considered.

Cybersecurity is a local, national and cross-border issue of common interest of the Europe and thus, the EU needs to have a thriving cybersecurity ecosystem, including industrial and research communities. The EU should start with accepting itself as cybersecurity universe, know what and where our weakness and strengths are, who we are missing in existing communities, how to complement and cater for a full spectrum, intertwined, multi-tiered and multi-layered ecosystem of ecosystems. It should for instance also be clear and continuously challenged, updated and improved, what such cybersecurity ecosystem and its communities should consist of, and how they should achieve and sustain future-proof European digital sovereignty.

The summary recommendations are illustrated herein with the details in deliverable D4.4.

CONCORDIA Cybersecurity Roadmap for Europe is a complex document. You can read its full version **here**. ←

# Influence the Cybersecurity Roadmap for Europe!

We created a brand-new tool that you can use for encoding your views. You can shape our roadmap by ranking challenges and recommendations or creating your ones. Your input will be valuable to our report on building the EU's resilience and digital sovereignty.

Have your say!

**concordia.monitorboard.nl/roadmap**

**Horizon 2020 Program (2014-2020)**
Cybersecurity, Trustworthy ICT Research & Innovation Actions
Security-by-design for end-to-end security
H2020-SU-ICT-03-2018