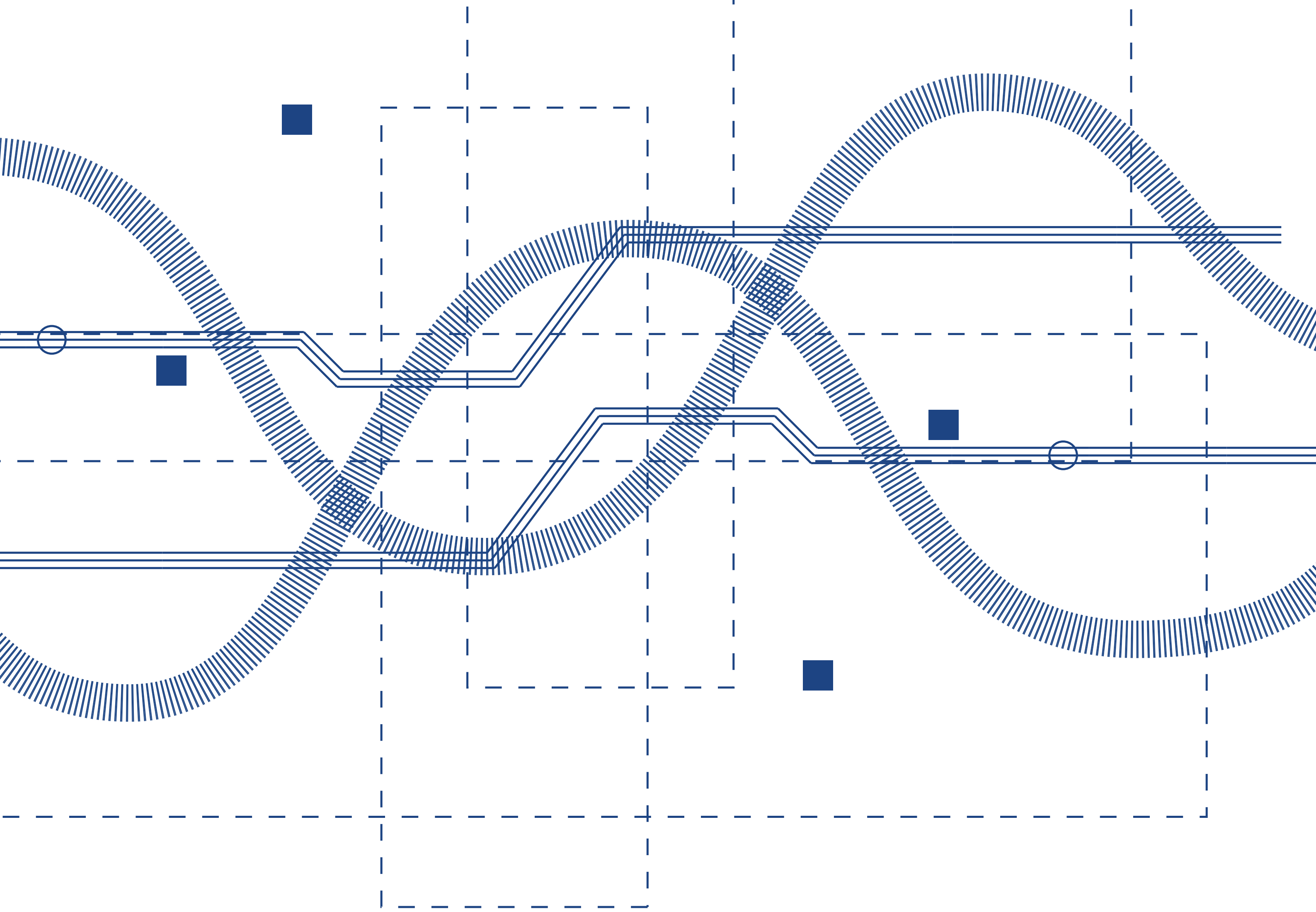
CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

Cybersecurity Roadmap for Europe

Introduction



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 2021.

1.1 Structure of the Document

The structure of the deliverable is as follows. It starts by motivating the CONCORDIA's holistic approach in defining the roadmap with a focus on six dimensions, 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 impact of COVID-19. The chapter concludes by listing technology stack-related recommendations. Chapter 4 focuses on the first dimension, 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 emerging aspects such as sustainability and green technologies. Additionally, each chapter summarizes the state of the art (SOTA) along with specific CONCORDIA contributions and, as relevant, the contributions to EU policy.

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

All future global market-dominant products, systems, and services will belocated 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 US 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 economical 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, organizations 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.

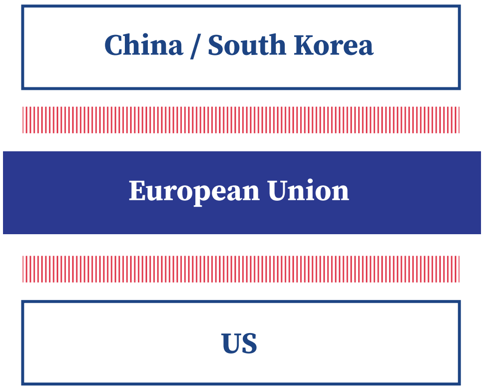


Figure 1: EU sandwiched between the US and China

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)**

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.

Please note, that this is a part of the CONCORDIA Roadmap. If you are interested in the whole document, you can download it ***here.***

[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*** (July 2020). Accessed Dec. 18, 2020.

[3] European Commission. ***Rethinking Strategic Autonomy in the Digital Age*** (July 2019). Accessed Dec. 18, 2020.

[4] European Union Agency for Cybersecurity (ENISA). ***Consultation Paper – EU ICT Industrial Policy: Breaking the Cycle of Failure*** (August 2019). Accessed Dec. 18, 2020.