Updated SPARTA SRIA (Roadmap v3)

Thomas Jensen

D3.4

Updated SPARTA SRIA (Roadmap v3)

Project number	830892
Project acronym	SPARTA
Project title	Strategic programs for advanced research and technology in Europe
Start date of the project	1st February, 2019
Duration	36 months
Programme	H2020-SU-ICT-2018-2020

Deliverable type	Report
Deliverable reference number	SU-ICT-03-830892 / D3.4 / V1.0
Work package contributing to the deliverable	WP3
Due date	February 2022 – M37
Actual submission date	31st May, 2022

Responsible organisation	INRIA
Editor	Thomas Jensen
Dissemination level	PU
Revision	V1.0

Abstract	This deliverable constitutes the SPARTA roadmap. It describes the SPARTA roadmap's mission statement of strengthening EU's digital autonomy via cybersecurity. To this end, a first step towards a prioritization of the existing program, transversal, and emerging cybersecurity challenges is provided with respect to their impact on digital sovereignty. The document outlines an open-source strategy, covering software as well as hardware, endorsed by SPARTA towards its mission. We also describe implications of the COVID-19 pandemic on cybersecurity and suggests recommendations to address them.
Keywords	Roadmap

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892.

Editor

Thomas Jensen (INRIA)

Contributors (ordered according to beneficiary numbers)

Philippe Massonet (CETIC)

Jan Hajný (BUT)

Marius Momeu, Sergej Proskurin, Mohammad Norouzian, Claudia Eckert (TUM)

Rios Velasco Erkuden (TEC)

Hervé Debar (IMT)

Ludovic Me, Guillaume Hiet, Thomas Jensen (INRIA)

Artsiom Yautsiukhin, Fabio Martinelli (CNR)

Evaldas Bruze (L3CE)

Michał Choraś, Marek Pawlicki (ITTI)

Reviewers (ordered according to beneficiary numbers)

Florent Kirchner (CEA)

Kadri Bussov (SMILE)

Executive Summary

This deliverable contains the final version of the updated SPARTA roadmap. In version V1 of the SPARTA roadmap we introduced the overarching mission of the roadmap and the process that governs its development. We also identified main challenges for further research and development activities. In addition to technology, we considered industrial, social, and economic aspects. We made special consideration of benefits for the EU and its strategic autonomy. During the creation of the initial roadmap, we took into consideration the already existing roadmap efforts at national and international levels in Europe. This allowed us to identify that the considered national cybersecurity roadmaps did not cover specific technologies, vertical sectors, and research domains of the JRC taxonomy. These findings helped us identify topics that were collectively disregarded in the past and thus potentially open up new directions. The comparison of our initial roadmap to the JRC taxonomy showed that the challenges we defined cover most of the crucial technologies, vertical sectors, and research domains. Our initial roadmap already emphasized that we can leverage the strength of EU countries in a wide range of expertise.

The SPARTA roadmap V2 was an updated version of V1, and represents a validation of the results achieved in previous versions. The initial roadmap was discussed thoroughly at SPARTA events with SPARTA partners as well as associates and interested third parties. As a result of these interactions, the identified challenges were confirmed as central topics. Based on this confirmation, we started the process of prioritizing the roadmap challenges with respect to the mission of strengthening digital autonomy in the EU. This prioritisation is based on input collected from the SPARTA network via an online survey conducted by the roadmap committee. Chapter 10 summarizes our major findings.

The COVID-19 pandemic has had an impact on our work on updating the roadmap. It has not been possible to hold workshops with physical participation since the Sparta Days in February 2019. Attempts have been made to replace such events by online formats, which are, however, significantly less effective in terms of interactivity. For this reason, various online questionnaires were designed by the roadmap committee in order to give the community alternative opportunities to participate in the roadmap developments. The aforementioned survey which we used for prioritizing the roadmap challenges leverages such an online questionnaire. However, COVID-19 has several other far-reaching consequences for cybersecurity. Due to the immense boost in digitization, which was accompanied by the rapid transition of working in home office environments and by the rapid transformation of business processes to distance economy, problems with maintaining cybersecurity became apparent. Therefore, we extended the SPARTA roadmap with Chapter 12 which gives several recommendations based on the lessons we learned on the cybersecurity implications for the EU. Specifically, we identify key societal and industrial areas where an increased risk on cybersecurity has been observed due to the pandemic, and we recommend ways to mitigate them.

During 2021, meetings have been held with the other cybersecurity network pilots (Concordia, Cybersec4EU, ECHO) and ECSO in a Roadmap focus group that has been coordinated by SPARTA. The outcome of these discussions has been concise description of key challenges that the four pilots and ECSO have identified. This document has provided input to the EU Cybersecurity Atlas and is reproduced in Chapter 13.

Table of Content

List of Figures

List of Tables

Chapter 1 Introduction

1.1 A roadmap for digital sovereignty in the EU

Digital sovereignty has emerged as a central objective in order to empower EU's strategic autonomy in the digital realm. This initiative is motivated by several observations:

- EU citizens and industries should be able to control and protect their personal data, in a digital environment where most cloud infrastructures are managed by non-EU providers.
- EU industries should remain at the forefront of innovation in the IT sector.
- IT products and services used throughout the EU should be certifiable, in accordance with key EU values such as trust and transparency.

The COVID-19 pandemic that started in 2020 has further contributed to demonstrate how dependable society is on reliable and secure digital infrastructures. As such, we describe in Chapter 12 a collection of cybersecurity issues observed to rise due to the pandemic along with recommendations on how to address them.

Cybersecurity plays a key role in ensuring digital sovereignty. To this end, the goal of the SPARTA roadmap is to analyze the scientific and technological cybersecurity challenges that must be met in order to strengthen the EU digital sovereignty and construct a secure and trustworthy digital single market across the Member States.

We have identified a number of frontier technologies where cybersecurity plays an important role and where continued investment is important in order to be at the forefront. The ordering has been realized based on input from the SPARTA network collected in a surveying campaign, during which we asked SPARTA partners, associates, and friends to prioritize the cybersecurity challenges from the present roadmap with respect to their impact on digital autonomy in the EU.

Under normal circumstances, we would have relied on in-person SPARTA workshops and events to stimulate the audience and gather feedback on the roadmap. However, since the past year has hindered such events, we performed the survey using an online questionnaire that we circulated virtually in the SPARTA network. We conducted this survey over the course of two months during which we received 19 submissions. Although we intend to enhance the analysis data by organizing more surveying campaigns in the following quarters, we have determined an initial prioritization based on the early submissions received so far. A complete analysis of the prioritization can be consulted in Chapter 10. According to the ranking, the top most critical cybersecurity challenges where the EU should elevate in order to come closer to digital sovereignty are:

- Secure and Fair Artificial Intelligence Systems for the Citizen
- Trustworthy Software
- User-Centric Data Governance
- Full-Spectrum Situational Awareness
- Education and Training

Nevertheless, the roadmap committee would like to underline that all cybersecurity challenges addressed in the present document are of high importance for achieving digital sovereignty in a sustainable manner.

In addition, we analyse the benefits that the open-source philosophy bring to cybersecurity and how open-source software and hardware can contribute to the goal of strengthening digital autonomy in the EU. As such, we propose an initial outline of a roadmap of open-source software and hardware cybersecurity technologies in Chapter 9.

The pandemic started in 2020 underpinned various aspects concerning cybersecurity of citizens, industries, and governments in the EU. Specifically, there is an increased risk in cybersecurity due

to the adoption of home-office and remote environments. As such, we introduce in Chapter 12 a collection of risks that we identified as increasing since the beginning of 2020. We established this selection based on, once again, input from the SPARTA network using the same mechanism as the aforementioned survey. Interestingly, we observed that most of the implications signalled by the pandemic are aligned with priorities towards digital sovereignty with a few differences. Thus, the COVID-19 pandemic has strengthened the importance of achieving this goal.

1.2 About this document

This document represents the efforts of partners in Work Package 3 (WP3) to establish a roadmap for research and innovation in European cybersecurity, leveraging the expertise of the consortium in technology, education and certification. Initially, the SPARTA partners defined 60 seed challenges in research and innovation addressing particular problems that they aim to solve within SPARTA. Out of these seed challenges, SPARTA launched four Programs that structure research activities within the SPARTA ecosystem. As these Programs are a well-rounded encapsulation for SPARTA research activities, their contents are used as one of the bases for our roadmap. We formulate long-term challenges based on the SPARTA Program plans, while also identifying new challenges that we consider essential in the future, called Emerging Challenges. Furthermore, we consider Europe's strengths and opportunities through previous roadmaps built at national and international levels. Apart from this, we consider newly identified strategic challenges important for the European research landscape. In addition, we provide a prioritization of all roadmap challenges with respect to their impact on SPARTA's mission to strengthen EU's digital sovereignty. We also introduce SPARTA's position towards open source hardware & software by outlining its benefits for security and how it influences our mission. Finally, we have added recommendations and lessons learned based on the operational changes introduced by the COVID-19 pandemic.

We begin by explaining the purpose of the SPARTA roadmap and the process used for its creation in Chapter 2. In Chapter 3, we analyse the landscape of national and international roadmap activities in European countries represented in SPARTA. Also, we relate the previous roadmap activities to the JRC taxonomy, which is one of the bases for the structure of our roadmap. This relation to the JRC taxonomy helps us to identify the similarities and differences between the areas that are considered important by different national and international roadmaps. In Chapter 4, we describe the template that we use to gather long-term challenges. This template contains a plethora of fields containing information about different technological, educational and certification parts of the challenges while considering economic and social aspects as well. This is also done having in mind the strengths, weaknesses, opportunities and threats that characterize these challenges within the European ecosystem. Chapter 5 contains a graphical representation of the roadmap, summarizing the information from all of the challenge tables and envisioned timelines to achieve the goals of tackling the Program Challenges, Transversal Challenges, and Emerging Challenges detailed in Chapter 6, Chapter 7, and Chapter 8. Chapter 9 sets the stage for an open-source roadmap for cybersecurity hardware & software. Chapter 10 presents the prioritization obtained from the SPARTA network for the roadmap challenges from the previous chapters. Then, Chapter 11 describes the relationship between the long-term challenges and the JRC taxonomy. Next, Chapter 12 presents various recommendations that the SPARTA network compiled based on the cybersecurity implications raised from the operational changes due to the Covid-19 pandemic. Finally, Chapter 13 concludes with an outlook on future work on this comprehensive roadmap.

Chapter 2 SPARTA Roadmap: Purpose and Process

2.1 The purpose of the SPARTA roadmap

The purpose of the SPARTA roadmap is to provide European decision makers and the European Commission in particular with mission-driven, strategic guidance for defining future projects and investments in cyber security. The objective is to close the cyber-skill gaps and prepare for future challenges, in both research, education and certification. The roadmap shall help to develop a mid-long term vision on cybersecurity related issues to cover emerging challenges, in alignment with the EC strategy for Horizon Europe.

The roadmap will operate with several levels:

- the **mission** of SPARTA (e.g., "securing the EU digital society"),
- the mission is structured into mission projects, in SPARTA these are called **programmes** (e.g., security of quantum information technology)**,**
- the **scientific challenges** of each programme that can be translated into a set of specific tasks with clearly identified, verifiable goals (e.g., post-quantum cryptography).

A list of "Grand Challenges" has been laid out by the commission of the EU (see https://ec.europa.eu/info/news/commission-launches-work-major-research-and-innovation-missions-cancer-climate-oceans-and-soil-2019-jul-04_en). These "Grand Challenges" are taken as external input to the roadmap of SPARTA.

The roadmap will be based on a clearly stated mission to be achieved. A mission should thus fill the gap between the Grand Challenges (e.g., the 17 Sustainable Development Goals, Societal Challenges, etc.) and concrete scientific and technological challenges. The mission of the SPARTA network is defined taking into account existing EU priorities such those formulated e.g. by ECSO for Horizon Europe and the Digital Europe Programme.

The mission of SPARTA will be defined to meet the following objectives:

- to build a secure digital society in Europe,
- to ensure European cybersecurity autonomy,
- to establish a trusted digital single market.

A programme has a clearly defined scientific and technological challenge and is divided into tasks for solving this challenge. Each program will achieve a number of scientific objectives. In this way, a mission provides the means to focus R&I and investments on solving critical problems.

The existing SPARTA Programs are:

- Full spectrum cybersecurity awareness,
- Continuous assessment in polymorphous environments,
- High-assurance Intelligent infrastructure toolkit,
- Secure and fair AI.

They come with a clearly identified research agenda, whose solution will contribute to the overall SPARTA mission. These programs are however only part of the whole "puzzle" and will be complemented by future programs that address complementary issues, including:

- next-generation architectures,
- network infrastructure,
- quantum communication and computation,
- …

Identification of new programs is part of the process presented below.

Each of the existing SPARTA Programs has its own program specific roadmap, defining tasks in terms of research, education and certification, and a time-line for achieving these tasks. These Program roadmaps are given in a later section in this document. An additional section provides a high-level description of the prospective programs

2.2 The SPARTA roadmap process

The SPARTA Roadmap design process is intended to be *agile*, considering emerging trends and technologies, and *open*, considering ongoing consultations with partners and associates in all partner countries. The Roadmap Committee leads the design of the SPARTA Roadmap. The role of the SPARTA Roadmap Committee is to coordinate, discuss, analyse and provide feedback on the input from workshops.

The roadmap is structured in accordance with the JRC taxonomy. Its evolution will involve monitoring EU and national initiatives and projects, and horizon scanning for emerging cybersecurity challenges. We can list a few important elements of the SPARTA Roadmap process:

- defining the SPARTA mission,
- identifying new programs and scientific challenges,
- reviewing and updating the SPARTA Roadmap.

The tools used in the roadmap process include:

- workshop with Associates and Friends,
- the SPARTA challenge form.

2.2.1 Defining the SPARTA mission

The SPARTA network should be guided by one, clearly stated mission. This mission should be defined taking inspiration from some of the greatest challenges facing our world, such as cancer, climate change, healthy oceans, climate-neutral cities and healthy soil and food. This list of challenges has been laid out by the commission of the EU, as described in the document on major research and innovation missions. (see https://ec.europa.eu/info/news/commission-launches-work-major-research-and-innovation-missions-cancer-climate-oceans-and-soil-2019-jul-04_en).

2.2.2 Identifying the programmes needed to accomplish the SPARTA mission

Experience from the American "Man on the Moon" mission in the 1960's emphasises the value of combining a clearly stated overall goal, defined top-down, with bottom-up experimentation to contribute to the overall success [1]. The SPARTA Roadmap will be established through a mixture of a bottom-up and a top-down approach. The division of the SPARTA mission will be defined in a top-down manner but will be based on input from the whole network, in a way similar to how the initial SPARTA roadmap was defined.

2.2.3 Identifying scientific/educational challenges to implement a programme

The implementation of a SPARTA Program will be done by addressing and solving specific scientific and technological challenges. These challenges will be identified in a bottom-up fashion, using the expertise of the partners of the network. In addition, the associates and friends in the network will be invited to provide new or updated challenges, which in turn will be reviewed and integrated by the

Roadmap Committee in the SPARTA Roadmap. This part of the process will rely on the Associates and Friends workshops, described below.

2.2.4 Roadmap review and revision

The SPARTA roadmap will be established through an iterative process that reviews and integrates the existing roadmap with respect to novel input from partners, associates and friends. A roadmap iteration involves the following sequence of steps:

1. Internal discussion in the SPARTA network of programmes and scientific challenges. This process is initiated and supervised by the Roadmap Committee.
2. Discussion with Associates and Friends in specially organised brain-storming workshops (described below)
3. Aligning the roadmap process between network pilots. Each of the four cybersecurity network pilots develops their individual roadmap. This step is intended to identify complementarity as well as synergies between these roadmaps in order to provide a coherent proposal to communicate to decision makers.

The SPARTA Roadmap is thus a living document that will be updated periodically throughout the duration of the project considering the latest technical, educational and societal developments, as well as identification of emerging programs.

2.2.5 Instruments of the SPARTA Roadmap process

2.2.5.1 The workshops with SPARTA Associates and Friends

The organisers of Associates and Friends workshops are encouraged to present the SPARTA Roadmap during the workshop and to give the audience the opportunity to provide feed-back on it. We foresee the session to include:

- feedback to existing programs,
- brain-storming to identify emerging programs.

The organisers are invited to keep

- minutes of the discussion that are to be shared with the programme committee,
- and identify interesting feedback that may lead to a SPARTA challenge/feedback.

2.2.5.2 The SPARTA challenge/feedback form

Feedback to the roadmap and identification of emerging challenges will be formalized in a "SPARTA challenge/feedback form", which may be updated/complemented over-time. This will be primarily used by programme committee to discuss updates to the roadmap, and keep track of the feedback provided. It will include:

- description feedback/emerging challenge
- submitter info (to get more info, and provide info on the status)
- responsible programme committee
- status (i.e. integrated, rejected, in-progress)

There will be an online form that is continuously available to allow stakeholders to provide feedback to the roadmap, or identify emerging challenges/programmes. In addition, results from a Sparta Associate and Friend workshops (see below) may provide basis for a SPARTA challenge/feedback form.

Chapter 3 Analysis of Strategic Research Agendas at National and EU Levels

In this section, we provide the results of our analysis of the current landscape in R&I in cybersecurity in Europe. In order to conduct our analysis, we looked for cybersecurity documents that influence the landscape on the national and European levels, identified the topics prioritized in the documents and mapped them into the taxonomy for cybersecurity R&I topics defined by the EU Joint Research Centre (JRC). Such an approach allows us to find the topics, which have already received attention as well as those that were not in focus in past years.

We want to underline that our analysis is focussed on the identification of the top priorities, rather than on ranking all possible topics. In other words, if a topic is considered important, but not a top priority, they may have very low (sometimes 0) score in our analysis. This should by no means be treated as the topic is of low (no) importance. In addition, our analysis is performed using the documents targeting civil research, which explains the low score for such an important application of cybersecurity technologies as Defence.

The validity of results depends on the quality of the selected documents. These documents were selected by the national partners who play a significant role in the R&I of the country and, thus, assumed to have good knowledge about the key documents shaping the R&I landscape in cybersecurity for a specific country. Furthermore, the partners of the SPARTA project have participated in many European roadmap activities (e.g., projects, various committees, European organizations, etc.) and have good knowledge of the key documents influencing European research funding programs (e.g., Horizon 2020). In summary, we conclude that the SPARTA partners have sufficiently broad expertise to select the best set of materials for the analysis.

3.1 Analysed documents

We have selected the following documents to be analysed at the national level:

- Austria: Austrian Cyber Security Strategy[1] (2013)
- Czech Republic: National Cyber Security Strategy[2] (2015)
- France:
  - Secrétariat du Conseil de l'Innovation: How to automate cybersecurity to make our systems permanently resilient to cyber attacks (2019)
  - INRIA: Cybersecurity. Current challenges and Inria's research directions[3] (2019)
- Germany: Selbstbestimmt und sicher in der digitalen Welt (Research program in federal government in IT security)[4] 2015-2020 (2015)
- Greece: Partners provided their input directly
- Italy: Libro Bianco (White Book)[5] 2018

[1] https://www.bmi.gv.at/504/files/130415_strategie_cybersicherheit_en_web.pdf
[2] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/cyber-security-strategy-of-czech-republic-2011-2015/@@download_version/48c136b4728d4a05aad610a436719ae0/file_en
[3] https://www.slideshare.net/INRIA/inria-cybersecurity-current-challenges-and-inrias-research-directions-131352245
[4] https://www.bmbf.de/de/sicher-in-der-digitalen-welt-849.html
[5] https://www.consorzio-cini.it/index.php/it/labcs-home/libro-bianco

- Lithuania: National Cyber Security Strategy[6] (2018)
- Luxembourg: National Cybersecurity Strategy III[7] (2018)
- Poland: The National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022[8] (2017)
- Spain:
    - Spanish Industrial Cybersecurity Roadmap 2013 - 2018[9] (2013)
    - INCIBE: Market Trends in Cybersecurity[10] (2016)
    -

We have selected the following documents to be analysed at the European level:

- NIS WG3 Strategic Research Agenda[11] (2015)
- ESCO: European Cybersecurity Strategic Research and Innovation Agenda (SRIA) for a contractual Public-Private Partnership (cPPP) v1.0[12] (2016)
- AEGIS: White Paper on Research and Innovation in Cybersecurity[13] (2018)
- NESSoS: D4.2 Part II: Engineering Secure Future Internet Services: A Research Manifesto and Agenda from the NESSoS Community[14] (2012)
- SYSSEC: The Red Book. A Roadmap for Systems Security Research[15] (2013)
- TDL: Strategic Research Agenda[16] (2012)
- Camino: D4.4 CAMINO roadmap[17] (2016)

3.2 JRC taxonomy

In order to compare various documents and identify the topics which have got most or less attention, we need a unique schema for comparison. In the scope of the SPARTA project, we used the recent JRC taxonomy[18] for cybersecurity research. The taxonomy is comprehensive enough and is focused on research and innovation in cybersecurity.

The JRC taxonomy was first published in 2018. We used this first version for the analysis of the various roadmaps that we describe in this section. The JRC later (November 2019) published an updated version of the taxonomy with minor modifications and additions to the three dimensions. In the list of the elements of the three dimensions, we present the added elements in italics.

[6] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf
[7] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/strategie-nationale-en-matiere-de-cyber-securite
[8] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/govermental-program-for-protection-of-cyberspace-for-the-years-2011-2016-2013/@@download_version/f28127b284314cc3b1ebec2946761ea9/file_en

[9] https://www.cci-es.org/documents/10694/0/Roadmap+CCI+English/998bbf3c-da70-4781-b40f-83d391f0cf85
[10] https://www.incibe.es/sites/default/files/estudios/cybersecurity_market_trends.pdf
[11] https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/strategic-research-agenda-draft-v02.63/at_download/file
[12] https://ecs-org.eu/documents/ecs-cppp-sria.pdf
[13] http://aegis-project.org/wp-content/uploads/2019/01/AEGIS-White-Paper-on-Research-and-Innovation-in-Cybersecurity.pdf
[14] https://cordis.europa.eu/docs/projects/cnect/0/256980/080/deliverables/001-NESSoSD41PartIIRoadmap.pdf
[15] http://www.chrismitchell.net/IY5512/Resources/syssec_red_book.pdf
[16] https://trustindigitallife.eu/wp-content/uploads/2016/07/TDL-SRA-version-2.pdf
[17] http://www.fp7-camino.eu/assets/files/Book-CAMINO_roadmap_250316.pdf
[18] http://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf

The JRC's taxonomy defines three dimensions for categorizing cybersecurity topics.

- Cybersecurity Research Domains;
- Application and Technologies;
- Sectors.

Cybersecurity Research Domain is focused on pure technological aspects of cybersecurity without concrete application. Application and Technologies (e.g., Robotics, IoT, Mobile, etc.) vector specifies various ICT Technologies which require cybersecurity protection. Sectors (e.g., Energy, Transportation, Healthcare, etc.) are different industries in which cybersecurity technologies are applied and which face sector-specific challenges.

Research Domains include the following topics:

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

The Technologies and Use Cases dimension contains the following topics:

- Artificial intelligence;
- Big Data;
- Blockchain and Distributed Ledger Technology (DLT);
- Cloud and Virtualisation;
- Critical Infrastructure Protection (CIP);
- *Protection of Public Spaces;*
- *Disaster resilience and crisis management;*
- *Fight against crime and terrorism;*
- Hardware technology (RFID, chips, sensors, routers, etc.)
- *High-performance computing (HPC);*
- *Human-Machine Interface*
- Industrial IoT and Control Systems (e.g., SCADA and CPS);
- Information Systems;
- Internet of Things; Embedded Systems; pervasive systems;
- Mobile Devices;
- Operating Systems
- Quantum Technologies
- Robotics;
- Satellite systems and applications;
- Vehicular systems;
- *UAV (unmanned aerial vehicles)*

The following Sectors are considered by JRC:

- Audiovisual and media
- *Chemical*
- Defence
- Digital Services and Platforms
- Energy
- Financial
- *Food and Drink*
- Government
- Health
- Manufacturing and Supply Chain
- Nuclear
- *Safety and Security of citizens and organisations*
- Space
- Telecomm infrastructure
- Transportation

In the end, we would like to underline, that JRC's set of Cybersecurity Technologies looks comprehensive, i.e., is supposed to cover all topics of cybersecurity, while Applications and Technologies and Sectors contain the most evident and essential topics, but hardly could be considered as a complete list (i.e., additional topics can be added if needed).

3.3 Analysis of results

3.3.1 National roadmaps

We have analysed the documents representing the national roadmaps and mapped them into the JRC's taxonomy to identify the topics, which have gained more/less attention currently. Table 1 shows the results of our analysis. Green cells represent the JRC's topics fully or partially covered in the corresponding document. Moreover, since National Cyber Security Strategies (NCSS) are by their nature and focus are different from industrial or research roadmaps; we use different colours (white country heading) to underline if an NCSS has been used to identify the priorities for the country. If we were able to identify a research or industrial roadmaps for the country, we used them and mark the corresponding country heading with grey colour. Finally, the available roadmaps have been ordered by the year of issue.

	Spain Ind.	Austria	Czech	Germany	Spain	Poland	Italy	Lithuania	Luxemburg	Greece	France INRIA	France	**Estonia**	**Poland**	**Spain**	**Greece**	**Czech**	**Luxemburg**	Total
	2013	2013	2015	2015	2016	2017	2018	2018	2018	2019	2019	2019	**2019**	**2019**	**2019**	**2020**	**2021**	**2021**	
Assurance, Audit, and Certification	■			■	■	■	■			■		■	■	■	■	■		■	12
Cryptology				■	■		■				■		■					■	6
Data Security and Privacy		■		■	■		■		■		■		■	■	■	■		■	11
Education and Training	■	■	■		■	■	■	■	■	■	■		■	■	■	■	■	■	16
Operational Incident Handling and Digital Forensics	■		■			■	■	■	■	■	■	■	■	■	■	■	■	■	15
Human Aspects				■	■						■						■		4
Identity and Access Management											■		■						2
Security Management and Governance	■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■	■	17
Network and distributed Systems				■	■	■							■		■			■	6
Software and Hardware Security engineering	■	■				■	■		■				■	■					7
Security Measurements	■								■	■					■				4
Legal Aspects		■	■					■		■	■		■	■	■	■	■	■	11
Theoretical Foundations																			0
Trust Management, Assurance, and Accountability				■							■								2

Table 1: Mapping of National Cybersecurity Roadmaps to JRC's Research Domains

The analysis shows that the following topics gained most attention recently. Note that two focus topics of SPARTA (*Education and Training* and *Assurance, Audit and Certification*) are highly ranked.

1. Security Management and Governance
2. Education and Training
3. Operational Incident Handling and Digital Forensics
4. Assurance, Audit, and Certification
5. Data Security and Privacy + Legal aspects

We see that, in contrast to other documents, such topics as *Human aspects, Cryptology* and *Network and Distributed Systems, Trust Management, Assurance and Accountability* are poorly covered by National Cybersecurity Strategies, mostly because they are too technical for this type of document.

If we go deeper into analysis of every domain, we find the following trends. The *Assurance, Audit, and Certification* domain gets high mostly due to the attention devoted to cyber security certification (topic of SPARTA's CAPE program). *Data Security and Privacy* clearly attracts more attention with new regulations which have come to force recently (e.g., GDPR). Countries recognise the need for rising cyber security awareness among citizens, improving security culture in the IT-dependent organisations, and augmenting the quality and quantity of skilled professionals in the cyber security field. Many national cyber security strategies explicitly mention cyber range (or other types of cyber security) exercises. Various activities for incidents reporting and sharing cyber security intelligence (the main topic of SPARTA's SHARK program) are facilitated at the country level (the most cited topic in *Operational Incident Handling and Digital Forensics* domain). The topics of Risk Assessment/Management and applying (and issuing new) cyber security standards is also frequently risen in the analysed documents (as examples of *Security Management and Governance*). Last, but not least, most countries recognize and pay significant attention to rising cyber security skills of their law enforcement agencies to be better prepared for fighting cyber crime.

With respect to changes in overall trends, we may see that *Operational Incident Handling and Digital Forensics* (mostly due to cyber threat intelligence sharing topic*)* and *Legal Aspects* have got a bit more attention in the latest years (2018-2021) with comparing to 2013-2017 period.

	Spain Ind.	Austria	Czech	Germany	Spain	Poland	Italy	Lithuania	Luxemburg	Greece	France INRIA	France	**Estonia**	**Poland**	**Spain**	**Greece**	**Czech**	**Luxemburg**	Total
	2013	2013	2015	2015	2016	2017	2018	2018	2018	2019	2019	2019	**2019**	**2019**	**2019**	**2020**	**2021**	**2021**	
Artificial intelligence;							■			■	■	■	■		■	■	■	■	9
Big Data;			■	■	■				■					■	■			■	7
Blockchain and Distributed Ledger Technology (DLT);							■				■		■		■			■	5
Cloud and Virtualisation;					■		■		■		■		■	■			■	■	8
Embedded Systems;					■				■			■							3
Hardware technology (RFID, chips, sensors, routers, etc.)																			0
Industrial Control Systems (e.g. SCADA);			■	■	■		■		■		■						■		7
Information Systems;											■								1
Internet of Things;			■		■		■				■				■	■	■	■	8
Mobile Devices;					■									■				■	3
Operating Systems																			0
Pervasive systems																			0
Quantum Technologies;				■			■										■	■	4
Robotics;							■				■				■				3
Satellite systems and applications;					■														1
Supply Chain;						■					■			■			■	■	5
Vehicular systems																	■		1

Table 2: Mapping of National Cybersecurity Roadmaps to JRC's Applications and Technologies

The following Applications and Technologies have the highest ranks in this analysis:

1. Artificial intelligence
2. Cloud and Virtualisation
3. Internet of Things
4. Big Data
5. Industrial Control Systems

Again, we see that the two topics of SPARTA's pilots SAFAIR and HAII-T (*Artificial Intelligence* and *IoT*) are among the first three. From this analysis, we see that some topics gain popularity: e.g., *Artificial intelligence* and *IoT*. At the same time the attention to SCADA systems falls (although cyber security in critical infrastructure is mentioned in almost all strategies). We also should underline the growing interest to *Blockchain and Distributed Ledger Technology* and *Supply Chain*.

	Spain Ind.	Austria	Czech	Germany	Spain	Poland	Italy	Lithuania	Luxemburg	Greece	France INRIA	France	**Estonia**	**Poland**	**Spain**	**Greece**	**Czech**	**Luxemburg**	Total
	2013	2013	2015	2015	2016	2017	2018	2018	2018	2019	2019	2019	**2019**	**2019**	**2019**	**2020**	**2021**	**2021**	
Audiovisual and media																			0
Defence									■				■	■			■	■	5
Digital Infrastructure													■	■	■	■	■	■	6
Energy					■		■		■	■									4
Financial					■		■		■									■	4
Government and public authorities							■						■				■	■	4
Health				■	■				■	■	■				■				6
Maritime																			0
Nuclear																			0
Public safety																			0
Tourism							■												1
Transportation				■	■		■		■					■			■		6
Smart ecosystems					■												■		2
Space									■									■	2
Supply Chain																			0

Table 3: Mapping of National Cybersecurity Roadmaps to JRC's Sectors

As for the Sectors, then the most cited are:

1. Healthcare/ Digital Infrastructure/ Transportation
2. Defence
3. Energy/ Financial/ Government and public authorities

Note that in this analysis we see the little contribution of National Cybersecurity Strategies since these documents often do not focus on the specification of the industries to be secured (and only vaguely outline the need to secure “Critical Infrastructures”, without properly defining the later term). We also should underline that *Digital Infrastructure* has been on a rise recently mostly due to security concerns of 5G technology and *Transportation* is often covered by security in automotive. Finally, we may see a slight increase in the attention to the government and public authorities’ networks.

3.3.2 European roadmaps

European roadmaps we analyse are those created in the scope of European projects or by European organizations to influence European research.

The top topics for cybersecurity research are:

- Security Management and Governance
- Data Security and Privacy
- Software and hardware security engineering
- Education and Training
- Security Measurements

Again, one of SPARTA's focus areas (i.e., Education) is one of the top topics, while Assurance, Audit and certification should follow next.

If we compare the results with the national roadmaps, we see that *Security Management and Governance* is still the top topic, as well as *Education and Training* and *Software and Hardware Security Engineering* are ranked high. On the other hand, we see more interest in the research community for *Data Security and Privacy,* and less attention given to the *Operational Incident Handling* and *Legal aspects*. However, we observe a slight increase in the documents mentioning *Operational Incident Handling,* which seems to indicate more interest devoted to the topic in the recent years. We connect this with increased information sharing activities, research devoted to more complex analysis of events coming from different sources (i.e., SIEM), as well as the application of Artificial Intelligence for the event analysis.

	NESSoS	TDL	SYSSEC	NIS WG3	cPPP	Camino	Aegis	Total
	2012	2012	2013	2015	2016	2016	2018	
Assurance, Audit, and Certification	■			■	■		■	4
Cryptology				■	■			2
Data Security and Privacy	■	■	■	■	■	■	■	7
Education and Training	■			■	■	■	■	5
Operational Incident Handling and Digital Forensics					■	■		2
Human Aspects	■		■	■	■			4
Identity and Access Management		■	■	■	■	■		5
Security Management and Governance	■	■	■	■	■	■	■	7
Network and distributed Systems	■			■	■		■	4
Software and Hardware Security engineering	■	■	■	■	■	■		6
Security Measurements	■	■		■	■	■		5
Legal Aspects		■						1
Theoretical Foundations				■	■			2
Trust Management, Assurance, and Accountability		■		■	■	■		4

Table 4: Mapping of European Cybersecurity Roadmaps to JRC's Research Domains

The top Applications and Technologies identified by the European roadmaps are:

- Mobile devices
- Big Data
- Cloud and Virtualization
- Blockchain and Distributed Ledger Technology
- Internet of Things
- Operating Systems

Mobile devices have much more attention to European roadmaps than National ones. In contrast, we see a reverse situation with IoT. One possible explanation of this could be that we have no so many recent (2018 and 2019) European roadmaps as we had National ones. On the other hand, such attacks as Mirai that raised significantly the importance of securing IoT outburst recently (about 2016).

Finally, we may also observe that the first four technologies (Artificial Intelligence, Big Data, DLT, Cloud and Virtualisation) are cited mostly in the recent documents.

	NESSoS	TDL	SYSSEC	NIS WG3	cPPP	Camino	Aegis	Total
	2012	2012	2013	2015	2016	2016	2018	
Artificial intelligence;							■	1
Big Data;				■	■	■	■	4
Blockchain and Distributed Ledger Technology (DLT);				■	■		■	3
Cloud and Virtualisation;					■	■	■	3
Embedded Systems;								0
Hardware technology (RFID, chips, sensors, routers, etc.)					■			1
Industrial Control Systems (e.g. SCADA);			■	■				2
Information Systems;					■			1
Internet of Things;				■	■		■	3
Mobile Devices;		■	■	■	■	■	■	6
Operating Systems		■		■	■			3
Pervasive systems								0
Quantum Technologies								0
Robotics;								0
Satellite systems and applications;								0
Supply Chain;								0
Vehicular systems				■				1

Table 5: Mapping of European Cybersecurity Roadmaps to JRC's Applications and Technologies

Finally, the top Sectors mentioned in various European roadmaps are as follows and are the same as the ones identified in the National roadmaps analysis:

- Healthcare
- Financial
- Transportation
- Energy

	NESSoS	TDL	SYSSEC	NIS WG3	cPPP	Camino	Aegis	Total
	2012	2012	2013	2015	2016	2016	2018	
Audiovisual and media								0
Defence								0
Digital Infrastructure		■			■			2
Energy	■			■	■		■	4
Financial		■		■	■		■	4
Government and public authorities				■	■			2
Health	■	■		■	■		■	5
Maritime								0
Nuclear				■				1
Public safety							■	1
Tourism								0
Transportation		■		■	■		■	4
Smart ecosystems				■	■			2
Space								0
Supply chain				■				1

Table 6: Mapping of European Cybersecurity Roadmaps to JRC's Sectors

3.3.3 Analysis of specific subtopics for JRC's Research Domains

In this section, we look deeper into the Cybersecurity Research Domains, considering the specific topics that have been cited most in both National and European documents. The reason for the united analysis is that 21 documents in total are still few for the detailed analysis of 150 subtopics. The precise mapping is not reported in the document because of its size.

Assurance, Audit, and Certification. There is a global consensus among the roadmaps concerning the need to progress in cybersecurity certification.

Cryptography and Cryptanalysis. There are no specific subtopics, which gained the most attention. In most cases, documents speak about cryptography in general without specification of the subtopic.

Data Security and Privacy. There are no specific subtopics, which gained the most attention.

Education and Training. Cybersecurity Education. *Cybersecurity Aware culture. Cybersecurity Exercises.* This topic is often covered in general as such, but also documents underline the importance of education and raising cybersecurity awareness. There is also an interest in a practical approach to education through cybersecurity exercises.

Operational Incident Handling and Digital Forensics. *Incident Response.* Much attention is devoted to the response to an incident. Moreover, the documents underline the importance of sharing information about the incidents and cybersecurity, as well as taking this information into account to increase the protection of the system.

Human Aspects. *Usability. Social Engineering.* Although Human Aspects did not get much attention, most problems outlined in the documents relating to the usability of security and preventing social engineering attacks.

Identity and Access Management. *Identification, Authorisation, Access control.* It is not surprising that those few documents that mention these topics speak about *Identification, Authorisation, and Access control.*

Security Management and Governance. *Risk management. Attacks and Threat modelling. Standards for Information Security. Incident management and disaster recovery. Reporting (e.g., disaster recovery and business continuity). Adoption, use, and continuance of information security technologies and policies. Attack prevention and detection.* This topic has come up frequently in our analysis of roadmaps. It covers many important aspects of cybersecurity. Each of these subtopics attracts attention, contributing to the overall sum of attention given to this topic.

Network and distributed Systems. There are no specific subtopics, which gained the most attention.

Software and Hardware Security engineering. *Secure software architectures and design. Vulnerability discovery and penetration testing. Malware analysis.* For this topic, the most interesting subtopics are those related to secure software engineering (security by design), the discovery of vulnerabilities and penetration testing, and analysis of malware.

Security Measurements. *Security metrics. The identification and application of suitable security metrics is the most frequently cited subtopic here.*

Legal Aspects. *Cybercrime prosecution and law enforcement. Cybersecurity regulation analysis and design.* The most cited legal aspects are related to cybercrime prosecution and analysis and the creation of new regulations.

Theoretical Foundations. There are no specific subtopics which gained the most attention.

Trust Management, Assurance, and Accountability. There are no specific subtopics which gained the most attention.

Chapter 4 Roadmap Challenge Template

SPARTA started with four programs that are summarized in the initial SPARTA Roadmap together with goals related to education and certification. However, the purpose of the roadmap was to go beyond the four programs, and identify emerging long-term challenges that are not yet covered by the four programs. To this end, the Roadmap Committee, considering the feedback from a diverse set of stakeholders, designed a SPARTA Roadmap challenge template. The template is used to describe long-term challenges and possible paths to their completion in Chapter 5. The template consists of three tables that are described in more detail in the following. The template represents a framework which helps to dynamically and incrementally extend the roadmap such that it can consider trends or challenges that will emerge in the future. Each challenge is described using the provided template that will be further incorporated in a timeline that will eventually become the final SPARTA roadmap.

For each challenge, the first table is structured in a way that provides a detailed description of the problem, trends, risks, and market opportunities. For this, it describes the status quo to identify state of the art and present the challenge from different aspects including research, industrial, and social aspect. Further, the template must outline the expected benefits for the EU for solving the particular challenge. Optionally, the table should have sufficient space to consider an in-depth SWOT analysis covering the *strength*, *weaknesses*, *opportunities*, and *threats* affecting the individual challenges. Finally, to establish a connection with prior work on the categorization of EU cybersecurity competencies, we take the dimensions of the JRC taxonomy into account. In case that emerging technologies could either benefit from the expected outcome of the challenge or influence research activities linked to the particular challenge, we also state them in a separate field.

Before introducing the subgoals of each challenge in detail, a figure gives a high-level overview of the challenge timeline. A timeline depicts the dependencies between the subgoals and an estimation of time needed for completion of each subgoal. The subgoals are divided into Technology, Education and Certification, wherein each challenge, multiple categories of subgoals can be present and interconnected.

Finally, the second table of each challenge details the subdivision in subgoals presented in the preceding figure. Each subgoal by itself is a representation of the technological activities that can be linked to the JRC taxonomy. By additionally aligning the individual subgoals to the remaining dimensions of the JRC taxonomy, *sector* and *domain*, it establishes a direct connection to this frame of reference. The descriptions of challenges and timelines reflect the current vision of members of the SPARTA Consortium.

Chapter 5 The Sparta Roadmap

This chapter summarizes the roadmap challenges, described in Chapter 6, Chapter 7, and Chapter 8, in a unified timeline of the SPARTA Roadmap to provide a general overview from a birds-eye perspective. The timeline combines the dimensions *technology*, *education*, and *certification* and aligns SPARTA's short- and midterm goals with these domains. The short- and midterm goals consider a timeline until the official end of SPARTA. Further, the timeline includes the project's as well as long term goals that go beyond SPARTA and will be pursued after the project's end. The goals are based upon the comprehensive feedback provided by SPARTA Programs and work package leads. The timeline further includes emerging challenges that are based upon the 60 initial challenges and challenges that have been identified by program partners during the execution of SPARTA. Figure 1 describes the timeline with final goals, establishing a long-term overview of the SPARTA roadmap. Figure 2 subdivides this broad overview of the goals into a detailed description of the subgoals of existing programs and other work packages. Figure 2 additionally shows a timeline with transitions as dependencies between stages that are envisioned as milestones during the work on achieving the final goals. The stages that are expected to be achieved during the development of SPARTA are shown for each year and the final goal is displayed at the end. For the emerging challenges of *Towards Secure Next-Generation Computing Architectures, Quantum Information Technology*, and *Trusted Hardware/Software Co-Design,* the expected year of completion is preliminary and dependent of a refined analysis of these challenges.

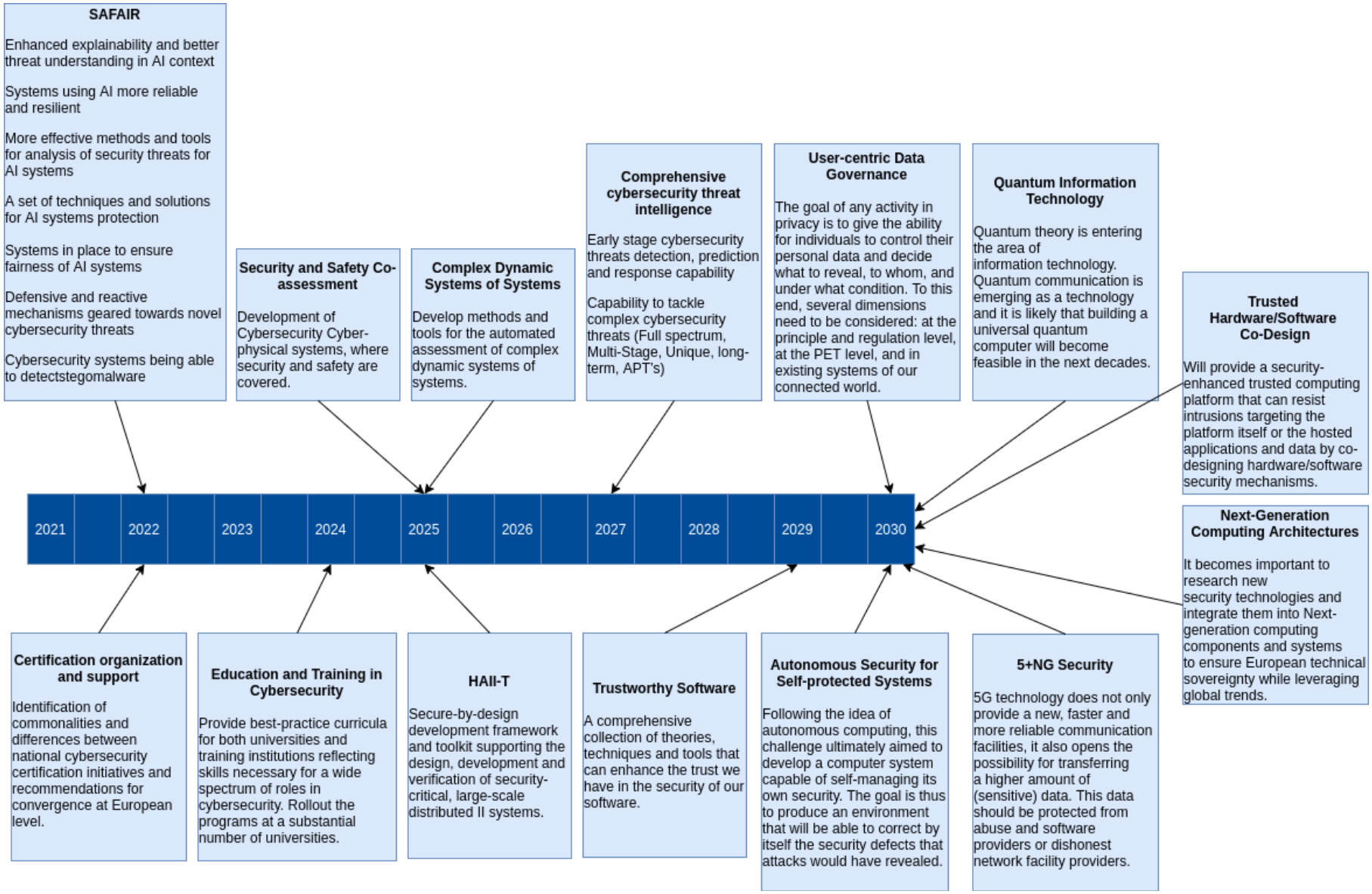


Figure 1: Roadmap with the final goals of solving the identified challenges

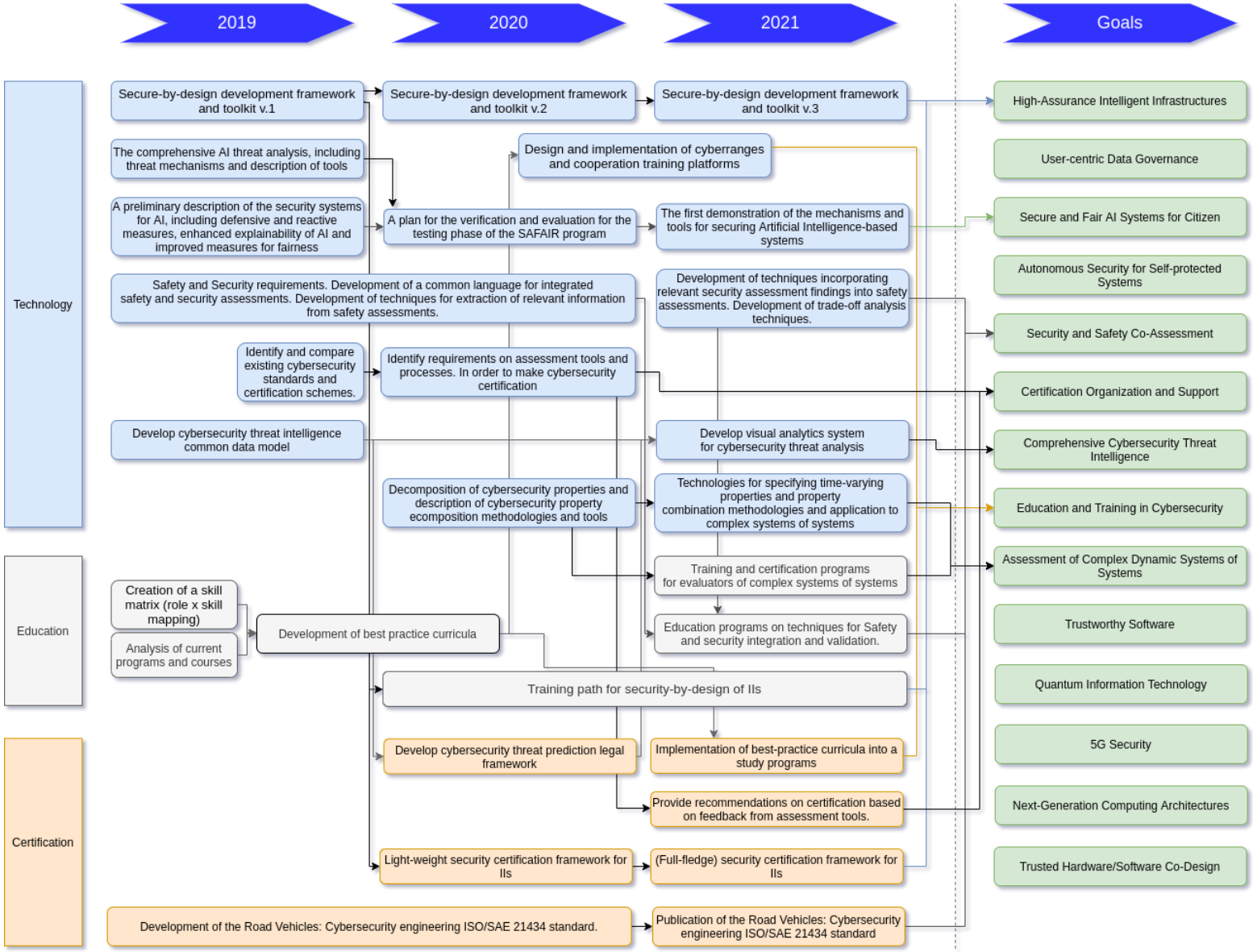


Figure 2: Timeline of stages for technology (blue), education (grey) and certification (orange) to meet SPATA challenges (in green)

Chapter 6 Program Challenges

In this chapter, we describe the challenges that the SPARTA working packages are tackling. This chapter contains long-term challenges identified from and related to the four SPARTA programs. While these challenges and their final goals are based on the four programs, they are not limited to the research plans for the SPARTA activity. Instead, they show a broader description and possible timeline of goals that would be important to complete as part of these challenges.

6.1 T-SHARK — Full-Spectrum Situational Awareness

Title: Comprehensive Cybersecurity Threat Intelligence

Problem description:

The problem definition is complex as the topic by itself:

- **Phenomena**: evolution and development of cyber-attacks and exploitation of different kinds of vulnerabilities have formed new categories of cyber-threats: complex by initial design, well planned, organized over the time by several stages, having good social engineering component, having political or ideological motives and/or linkage with high value industrial or geopolitical gains. New, high complexity, threats require new approaches and methods on how to tackle them.
- **Approach**: for more complex, multi-stage, full-spectrum cybersecurity incidents traditional cybersecurity function organization is not sufficient and not effective anymore. Considering this part of phenomena, detected cybersecurity incidents (ones being part of the large multistage operation), puts us in the situation where we can only fight consequences. We need capabilities to fight phenomena on early phases of multi-stage operations, meaning – moving from incidents to threats, from reactive to predictive organization of cybersecurity.
- **Governing cybersecurity:** to address complex, multi-stage, full-spectrum, uniquely designed cyber-attacks, cybersecurity must be organized cross-institutionally and cross-border. Single institution perimeter protection-oriented cybersecurity organization is not efficient and does not provide sufficient context information in order to spot correlation, make a prediction and decide on adequate measures on early stage. We need to bring cybersecurity towards a collaborative organization.
- **Data sharing:** collaborative organization of cybersecurity naturally requires wider data access and data/information sharing, which is challenge by itself. GDPR and other privacy, security and confidentiality
- **Concept**: historically organization of cybersecurity function had more technical roots and IT perimeter security organization. Nowadays, cybersecurity is an important piece of differently targeted attacks and requires a comprehensive approach to uniting both societal and technological sides of threats to tackle them. Such an operation like Elections Interference is a combination of direct attacks, public brand and reputation attacks, information lacking, fake news, propaganda, the polarization of society, etc. Social engineering plays therefore an ever more significant role in cyber threats.
- **Analysis model**: diverse cybersecurity information and indicators of threats are hardly incorporable into a single analytical model. Empirically we can state that in such a situation, visual analytics techniques are the way to solve it; however, which one is the most efficient for cybersecurity threats is an open question for now.
- **Regulatory:** organizing cybersecurity function around early phases of the kill chain

raises many regulatory questions and demands: how to define the threat, how to measure it, which privacy, ethical and other standards should be applied in order to maintain the balance between enforcement and individual rights.
- **Legal:** tackling the cyber threats – which legal framework should be applicable for the process, especially considering globality of the phenomena – most of the top tier threats are coming from abroad and originate from outside the EU.

Final goal:

Comprehensive cybersecurity threat intelligence

- Early-stage cybersecurity threats detection, prediction and response capability
- Capability to tackle complex cybersecurity threats (Full spectrum, Multi-Stage, Unique, long-term, APT's)

Status Quo:

- **Europe:** inside the EU, several industrial players as well RTO's and academic institutions are working on separate components enabling one or another feature of the desired solution
- **International:** similar solutions can be found in national-level implementation in the USA, as well some of USA originated solutions, like Recorded Future, provides platform covering most of the aspects for analysis.

Estimated year of completion: expected time 2027

Research aspect:

- Building comprehensive cybersecurity threats situational awareness picture
- Visual Analytics methods applied for comprehensive cybersecurity threats analysis
- Different origination and nature data sharing among diverse actors
- Cybersecurity threats analysis regulatory framework
- Legal basis for comprehensive cybersecurity threat processing
- Ethical issues (related e.g. to the broad monitoring of communications and censorship aimed at fighting fake news).

Industrial demand:

- Need for EU proprietary tools, technologies and solutions to assure top tier cybersecurity threats prevention.
- Potential application in automotive, energy, critical infrastructure sectors

Social aspect:

- General need to ensure the public safety of democratic processes inside the EU (avoiding Elections Interference and other negative ideology-driven societal impacts)
- More informed and trusted decision-making process in cybersecurity

Benefit for EU:

- EU cybersecurity institutions will have capabilities to address complex, advances cyber threats
- EU institutions will have the knowledge and capabilities to work with cyber threats (early phases of kill chain)

• Solutions developed in a targeted timeframe will put EU industries, SME's, Academia into the lead position in this field.

SWOT Analysis:
- **Strengths:**
  - Meeting actual demand
  - Realistic to implement and achieve
  - High support by end-users
- **Weaknesses**:
  - Demands for large scale information access
  - Organized around the "Threats" concept, that is new and has little of regulatory and legal frameworks
- **Opportunities**
  - Is ambitious and gives long term perspective to take leading positions in the global market
  - New niche
  - High market demand and high market scale for commercialization
- **Threats**
  - Many of innovative aspects tipping together that increases the risk of failure

Domain (JRC Taxonomy): Top-Tier Cybersecurity Threats
Sector (JRC Taxonomy): • Defence, Governmental and public authorities, Public Safety as direct sectors • NB! All other sectors are also relevant, but may not be seen as primary end-users • Impact Example: elections' interference
Relation to Emerging Technologies: • Threats intelligence • All-data based analytics • Visual analytics • Predictive analytics of cyber threats

Table 7: General information for Comprehensive Cybersecurity Threat Intelligence (from T-SHARK)

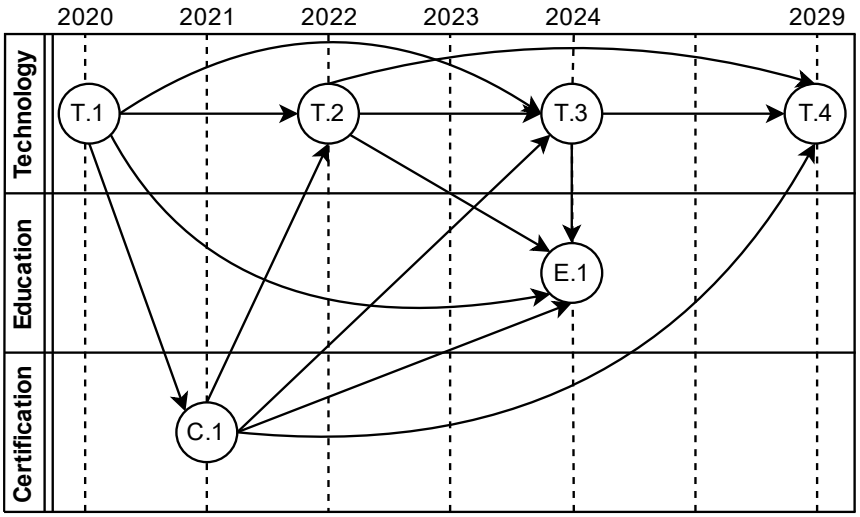


Figure 3: Timeline for the expected completion of subgoals for Comprehensive Cybersecurity Threat Intelligence (from T-SHARK)

Stage/Dimension	Sector (JRC)	Domain (JRC)	Regulation
T1	Public Safety, Government and Public Authorities, Defence, Smart ecosystems	Data Security and Privacy, Networks and Distributed Systems, SW and HW Security Engineering, Theoretical Foundations	A flair for sharing - encouraging information exchange between CERTs,
	Description (incl. obstacles): Develop Cybersecurity threat intelligence common data model To make this shift, decision makers and cybersecurity practitioners should be equipped with structured information, allowing them to gain High Awareness and Full Picture on different time dimensions (Current, Near Future and for more complex attacks - Far Future). This information includes much wider scope than current/upcoming incidents and information, describing them (technical information and beyond to some extend). The initiative aims to build the first block of the desired shift by developing model of information provision (incl.: information structure, sources, process, actors and their roles, etc.) facilitating High Awareness and Full Picture, leading to Awareness based Cybersecurity. It will also lead changes in the scope of the information used. To enable the shift, cybersecurity threat intelligence must be extended and enriched with the related external information and information from other security domains, as well general context information that would allow performing Full Spectrum Analysis of potential and evolving		

<table>
<tr><td></td><td colspan="3">threats. The scope of information used for comprehensive cybersecurity threat analysis will vary from case to case, but it is much wider than it would be possible to collect from technical infrastructure indicators. Therefore, development of an extended common data model for integrated cybersecurity threat intelligence is the key.

Obstacles:

• How to create the data model that would support both – technical incidents data and general context data at the same time allowing to transfer information from OSINT and Information Security fields.
• How to collect comprehensive cybersecurity threats data (information) that is relevant for full spectrum analysis of cybersecurity incidents and evolving threats?
• How to integrate data (information) of different nature, types, and structures into “Comprehensive Cybersecurity Threat Intelligence Monitor” in the vivid and actionable manner?
• How to define (and limit where possible) the “right” volumes of data used during more complex risk and threat intelligence processes, in a way which will balance the need to know as much as possible and assure the highest prevention of private and unnecessary data usage for the intelligence purposes.
• How to effectively manage large volumes of data used during more complex risk and threat intelligence processes.</td></tr>
<tr><td rowspan="2">T2</td><td>Public Safety, Government and Public Authorities, Defence, Smart ecosystems</td><td>Data Security and Privacy, Networks and Distributed Systems, SW and HW Security Engineering, Theoretical Foundations</td><td></td></tr>
<tr><td colspan="3">Description (incl. obstacles):

Develop Visual Analytics System for Cybersecurity threat analysis

Integration of various type of data and early hypothesis building, as well insights generation is key for predictive cybersecurity function organization. New evolving type of analytical techniques having high adoption for High Situational Awareness development as well Decision-Making Process Support in Visual Analytics techniques.

Obstacles:

• High diversity of data types and formats
• Different means of data by granularity and source
• Exposure of information while maintaining data confidentiality and security policies</td></tr>
<tr><td>T3</td><td>Public Safety, Government and Public Authorities, Defence, Smart</td><td>Data Security and Privacy, Networks and Distributed Systems, SW and HW</td><td></td></tr>
</table>

	ecosystems.	Security Engineering, Theoretical Foundations	
	Description (incl. obstacles): Develop cybersecurity threat analysis model. For the cybersecurity the analysis model in majority of the situations is precedent and factual information analysis driven. However, to handle large scale and critical incidents is not enough and sometimes even too late to have reactive organization of cybersecurity function. For this subset of cybersecurity topic, preventive organization of the cybersecurity function is required, making it necessary to move from incident towards threat. However, threat is not a fact-based incident but more likelihood- and assessment-based, - rather dependent on the context and attributes influencing it. Therefore, analysis model should be extended and adopted to reflect this and other differences. **Obstacles:** • Clear definition of cybersecurity threats and how to identify them • Analysis model to forecast likelihood of the threat to happen and trending curve (increasing or not) • More complex threats have wide influencing context. Question is how to integrate complete context, as the raw data is managed by several institutions, sometimes even cross-boarder.		
T4	Public Safety, Government and Public Authorities, Defence, Smart ecosystems	Data Security and Privacy, Networks and Distributed Systems, SW and HW Security Engineering, Theoretical Foundations	EC, Joint Communication to the EP and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 2017 A Global Strategy for the EUFSP, 2016
	Description (incl. obstacles): Develop comprehensive full-spectrum cybersecurity threat intelligence methodology Properly applied full spectrum cybersecurity threat intelligence can provide greater insight into cyber threats, allowing faster, more targeted response and better resource development and allocation. For instance, it can assist decision makers in determining acceptable risks, developing controls, planning budgets, making equipment and staffing decisions (strategic intelligence), provide insights that guide and support incident response and post-incident activities (operational/technical intelligence), and advance the use of indicators by validating, prioritizing, specifying the length of time an indicator is valid (tactical intelligence). In other words having a more complete		

<table>
<tr><td></td><td colspan="3">situational picture on all levels of threat Intelligence and comprehensive understanding of the potential and evolving threats allows cybersecurity managers to cut through the noise of technical security incidents and focus on the threats most likely to have a major impact on business and assets under their protection, to make right decisions how to respond to ongoing incidents.

At the same time, it is necessary not only to respond to the known incidents and threats but also work on those that are out of reach of our knowledge. In this task, computer technology developers have recently introduced series of different artificial intelligence, machine learning and other cognitive computing solution, which would be very helpful for cybersecurity industry as well.

The facilitated shift (organic shift will take longer and will always fall behind quickly evolving cyber threats) of cybersecurity activities within the responsible institutions to the awareness-based activities is supported by different theories. Some to be mentioned, are:
• Bloom’s theory on the depth of knowledge and perception;
• Organization learning theories (e.g. Learning curve);
• Field theory by Kurt Lewin;
• Decision making theories (e.g. prescriptive decision theory, SDM theories)

Obstacles:
• Absence of robust and up to date cyber threats taxonomy, that would enable threats categorization and countermeasures planning addressing complexity of attack types, actors, goals, impact, motivation, longevity, perception.
• Cybersecurity was seen as technological discipline and lacks integrity with social science into one comprehensive cybersecurity intelligence methodology.
• Incidents based cybersecurity function is more linear process working with factual information, however threats are more iterative process working with probabilities and dynamic aspects of phenomena. New know-how also need to be developed and systematized in this area.</td></tr>
<tr><td>E1</td><td>Public Safety, Government and Public Authorities, Defence, Smart ecosystems</td><td>Data Security and Privacy, Networks and Distributed Systems, SW and HW Security Engineering, Theoretical Foundations</td><td></td></tr>
<tr><td></td><td colspan="3">Description (incl. obstacles):

Education programs on the basis of comprehensive full-spectrum cybersecurity threat intelligence methodology.

All of technical and methodological developments and inventions, must be integrated into existing education and training programs to ensure sustainable capability development and ensure smooth transition to</td></tr>
</table>

<table>
<tr><td></td><td colspan="3">new competence structure.
Obstacles:
Very diverse multi-disciplinary competence required to address the goal
New and constantly evolving phenomena having high dynamics increases complexity of the</td></tr>
<tr><td rowspan="2">C1</td><td>Public Safety, Government and Public Authorities, Defence, Smart ecosystems</td><td>Data Security and Privacy, Networks and Distributed Systems, SW and HW Security Engineering, Theoretical Foundations</td><td>Directive 2013/40 on attacks against information systems, Directive 2013/37 on the re-use of public sector information, General Data Protection Regulation 2016/679, the Police Directive 2016/680, the NIS Directive</td></tr>
<tr><td colspan="3">Description (incl. obstacles):
Develop cybersecurity threat prediction legal framework
Existing legal framework have developed over the years to address cyber incidents perspective of the process. However, moving towards early stages of the kill chain and extending preventive aspects of cybersecurity function requires extension (or adoption) of legal framework to address not the incident-based but threat-based legal organization. At the same time, it should reflect recent evolution of cybersecurity threats – becoming even more global and complex.
Obstacles:
Not clear definition of the Threat in cybersecurity legal framework
Globality of the phenomena – international and various national laws intersecting in most of the cases.
Effective measures for the top tier threats coming from abroad and originating outside the EU (non reachable from prosecution perspective)</td></tr>
</table>

Table 8: Detailed description of Comprehensive Cybersecurity Threat Intelligence (from T-SHARK)

6.2 CAPE — Continuous Assessment in Polymorphous Environments

Differently to the other programs, the CAPE program is providing its input to the roadmap along with two separate challenges. This is because the two aspects of the program have very different expectations. The first one focuses on complexity and dynamicity of IT systems of systems, where the main issue is to adapt assessment processes to dynamicity and complexity. The second one focuses on resilience of the physical world, embedding both security and safety features into physical components controlled through IT processes.

The two challenges are felt sufficiently different at this stage to provide separate roadmap descriptions, even though both may be found in a single use case. Future versions of the roadmap may fuse both roadmaps if strong convergence emerges during the execution of the program.

6.2.1 Security and Safety Co-Assessment (from CAPE)

Title: Security and Safety Co-Assessment

Problem description: Systems and services are increasingly relying on connectivity for operations, typically command and control. This means that if adequate counter-measures are not put in place, these systems may be vulnerable to cyber-attacks that can cause catastrophic events, e.g., human and environmental losses. In order to prevent these events, it is necessary to ensure that safety properties are not adversely impacted by a cyber-attack. Therefore, it becomes necessary to include cybersecurity properties in the specification and assessment of safety properties. In the automotive domain, the deployment of applications and services must include security and privacy requirements to protect critical functions such as driver assistance, collision warning, automatic energy braking, and vehicle safety communications. Cyber-attacks on these functions can cause accidents and therefore, shall be avoided, while still maintaining the safety of the system. This is a necessary step towards the deployment of trustworthy autonomous/automated vehicles.

Final goal: Development of Cybersecurity Cyber-physical systems, where security and safety are covered.

Status Quo:

- **Europe:** Several research groups are pursuing research in safety and security. Several projects like AMASS [4], EMC2 [5] and MERGE [6] develop model-based solutions for safety and security assurance, i.e., compliance demonstration, safety-security co-engineering, and compositional assurance of security and safety aspects. Different approaches for the trading between safety and security requirements are pointed out as well. Regarding co-analysis techniques, the FMVEA technique is deeply investigated in [7].
- **International:** Nowadays, different standardization approaches w.r.t. safety and security concerns exist. Those standards address the system development life-cycle not only from the perspective of safety concerns but also from security. Especially, the aspects of security which impact on safety are tackled. Moreover, these recent standards promote safety and security co-engineering. Nowadays, the most important security standard is the ISO/SAE 21434 recently published which specifies engineering requirements for cybersecurity risk management regarding concept, product development, production, operation, maintenance and decommissioning of electrical and electronic (E/E) systems in road vehicles. Other two remarkable standards are IEC 62443 for industrial automation, which gives guidance on how security threats for safety-

critical control systems shall be treated and the SAE J3061 standard, which defines a safety and security interaction point approach corresponding to the automotive functional safety standard ISO 26262.
Estimated year of completion: 2025
Research aspect: Common languages for safety and security; detection and management of conflicting between safety and security requirements; tools for assessment and certification. Process(es) for safety and security co-engineering. Methods for gathering evidence supporting the compliance of safety and security assessment; Ensuring that security solutions are embedded in the system design to support the concept of 'security by design'.
Industrial demand: All industrial/critical infrastructure and cyber-physical systems, in general.
Social aspect: Trust in components that are used daily, such as vehicles, building management systems, transportation, energy, telecommunication, health, manufacturing, etc.
Benefit for EU: Develop trusted components for the Digital Society. Ensure that certifications schemes meet EU needs and values.
SWOT Analysis: - **Strengths:** Existing research activities in the EU - **Weaknesses:** Conflicts between safety and security requirements, difficulties in trade-off development, need for better integration between security and safety, the specificity of the solution to the use cases - **Opportunities**: Concrete guarantees for safety and security, certain use cases (e.g., connected vehicle) are applicable to major industries in Europe - **Threats**: Major actors in the digital transformation (GAFAM) are developing and experimenting with these technologies
Domain (JRC Taxonomy): Theoretical Foundation, Human Aspects, Legal Aspects, Data Security
Sector (JRC Taxonomy): Transportation, Health, Energy, Financial, Government, etc.
Relation to Emerging Technologies: Connected vehicle, smart mobility (building, city, transportation), collaborative robots.

Table 9: General information for Security and Safety Co-Assessment (from CAPE)

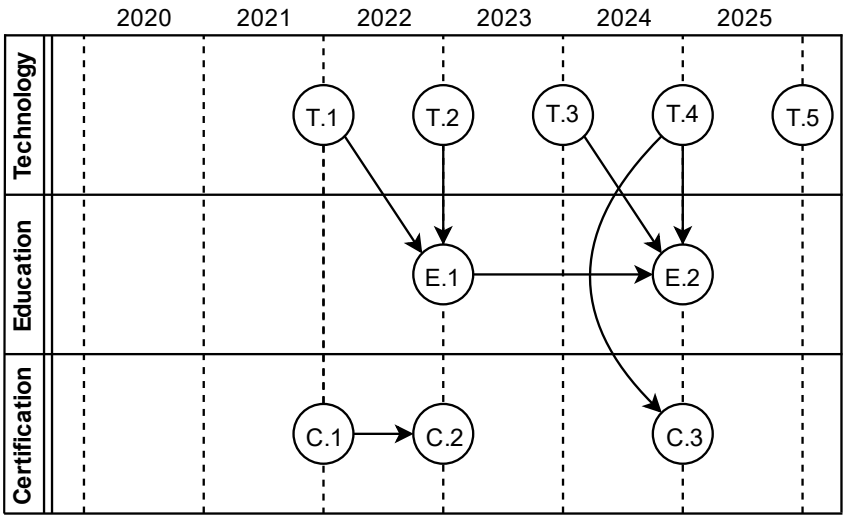


Figure 4: Timeline for the expected completion of subgoals for Security and Safety Co-Assessment (from CAPE)

Stage/Dimension *Tx for Technology* *Ex for Education* *Cx for certification*	**Sector (JRC)**	**Domain (JRC)**	**Regulation**
T1	Energy, Financial, Government and Public Authorities, Health, Transportation, Smart ecosystems.	Education and Training	
	Description (incl. obstacles): Safety and Security requirements Development of a common language for integrated safety and security assessments. Development of techniques for the extraction of relevant information from safety assessments.		
T2	Energy, Financial, Government and Public Authorities, Health, Transportation, Smart ecosystems.	Education and Training	
	Description (incl. obstacles): Development of techniques incorporating relevant security assessment		

<table>
<tr><td></td><td colspan="3">findings into safety assessments.
Development of trade-off analysis techniques.</td></tr>
<tr><td rowspan="2">T3</td><td>Energy, Financial, Government and Public Authorities, Health, Transportation, Smart ecosystems.</td><td>Data Security and Privacy, Networks and Distributed Systems, SW and HW Security Engineering, Theoretical Foundations</td><td></td></tr>
<tr><td colspan="3">Description (incl. obstacles):
Development of safety and security co-verification and validation techniques.

Description: The gathering of concrete evidence supporting the dependability (safety and security) assessment is essential to ensure that the developed artefact complies with the analysis. In particular, one needs to validate that the trade-off analysis carried out during the assessment phase are reflected in the artefact. For example, validate that the counter and control mechanisms places interfere without invalidating the assessment phase. Similarly, verification techniques shall be placed to check for defects or vulnerabilities that can be exploited by attackers to cause hazards. Co-verification has to, therefore, exploit the architecture placed, e.g., safety patterns, to guide the verification of defects that can be exploited by attackers.

Obstacles: Dependability assessments may not be detailed enough to improve the type of co-verification and validation methods.</td></tr>
<tr><td rowspan="2">T4</td><td>Energy, Financial, Government and Public Authorities, Health, Transportation, Smart ecosystems.</td><td>Data Security and Privacy, Networks and Distributed Systems, SW and HW Security Engineering, Theoretical Foundations</td><td></td></tr>
<tr><td colspan="3">Description (incl. obstacles):
Develop incremental methods for safety and security integration.

Description: With the increased connectivity of vehicles, new features can be installed to systems even after production. These features may require the integration of safety and security. However, instead of re-assessment the whole system, such incremental changes to the system shall only require incremental re-assessments, thus not requiring repeating unnecessarily verification and validation tasks.</td></tr>
</table>

	Incremental methods, however, still shall guarantee the safety and security of the system that is updated. **Obstacles**: The degree of incrementality may not enable techniques to re-use parts of the assessments.		
T5	Energy, Financial, Government and Public Authorities, Health, Transportation, Smart ecosystems.	Data Security and Privacy, Networks and Distributed Systems, SW and HW Security Engineering, Theoretical Foundations	
	Description (incl. obstacles): Continuous safety and security assessment process **Description**: The dependability (safety and security) of systems shall be guaranteed throughout their life-cycle. This means that the dependability assessment of these systems shall be re-evaluated whenever there is a change in the system or a new fact is discovered, e.g., new cyber-attacks. This becomes even more relevant with the increase in the number of autonomous and automated features available in vehicles. The continuous assessment process shall be supported by automated techniques that among other things develop an argument supporting the safety and security of systems; the gathering of evidence from sources possibly distributed around the globe demonstrating that the system complies with the argument by, for example, deploying validation and verification tools/techniques. **Obstacles**: Such a continuous process will depend on the technologies available, e.g., the verification tools, underlying communication secure channels assumptions, and distributed evidence storage. This may require centralized entities that manage the process.		
E1	Energy, Financial, Government and Public Authorities, Health, Transportation, Smart ecosystems.		
	Description (incl. obstacles): Education programs based on Safety and Security assessment.		
E2	Energy, Financial, Government and		

	Public Authorities, Health, Transportation, Smart ecosystems.		
	Description (incl. obstacles): Education programs on techniques for Safety and Security integration and validation.		
C1	Transportation, Smart Ecosystems	Data Security and Privacy; Assurance, Audit and Certification	
	Description (incl. obstacles): Publication of the Road Vehicles: Cybersecurity engineering ISO/SAE 21434 standard.		
C2	Transportation, Smart Ecosystems	Data Security and Privacy; Assurance, Audit and Certification	
	Description (incl. obstacles): Update of the Road Vehicles: Cybersecurity engineering ISO/SAE 21434 standard		
C3	Energy, Financial, Government and Public Authorities, heath, Transportation, Smart ecosystems.	Data Security and Privacy; Assurance, Audit and Certification	
	Description (incl. obstacles): Implementation of the UNECE Regulation No 155 and No 156.		

Table 10: Detailed description of Security and Safety Co-Assessment (from CAPE)

6.2.2 Complex Dynamic Systems of Systems (from CAPE)

Title: Assessment of Complex Dynamic Systems of Systems
Problem description: IT services are increasingly complex and dynamic, as exemplified by the DevOps paradigm. They also increasingly rely on third-party services, either transparently (such as name resolution or routing at the network level), or explicitly (such as single sign-on

provided by major Internet actors to smaller entities). On the other hand, assessment and certification processes are static, long and expensive. Therefore, it becomes increasingly difficult to evaluate and certify interdependent complex systems that constantly evolve and receive new functionalities. This implies that the target of evaluation is undergoing constant evolution.

The challenge is to 1) define and publish the appropriate cybersecurity properties; 2) assess that these properties are met by increasingly complex and dynamic systems and services; 3) certify compliance with these cybersecurity properties as well as regulations, in a way that is verifiable by providers and customers alike. This must happen all along the lifecycle of these products and services, from design to retirement. It must be robust to either runtime changes or lasting modifications, ensuring that assessment (and certification) evolves at the same pace as services.

The focus of this challenge is on cybersecurity for complex digital infrastructures, offering e-services. Even though these digital infrastructures might be driven by physical processes, safety and resilience aspects are treated in the second challenge of the CAPE program.

Final goal: Develop methods and tools for the automated assessment of complex dynamic systems of systems.

- Assessment automation
- Adaptation of assessment procedures to runtime dynamic behaviour
- Assessment of service interdependencies

Assessment towards certification of systems and services

Status Quo: Digital services are deployed at an increasingly fast pace, without the associated validation and certification, putting services in a chaotic state and reducing trust and use

- **Europe:** EU research funding has supported many efforts related to the development of secure IT components (e.g., authentication, detection, etc.) and services, particularly cloud services; however, evaluation and assessment of research results and products remain essentially through certification of individual components.

International: Similar efforts have been led outside of Europe. For example, several datasets have been published all over the world for the assessment of intrusion detection systems.

Estimated year of completion: 2025 to 2027

Research aspect:

- Modelling of the properties of complex systems
- Automated assessment methods and tools
- Incremental assessment methods and tools

Industrial demand: Automation of assessment and certification, leading to better stability of systems and services, as well as non-regression.

Social aspect: Better stability of systems and services, leading to increased trust and use.

Benefit for EU: Support to the development of EU-based champions; better management of

the supply chain when sourcing products and services outside of the EU, to better support European requirements and values.
SWOT Analysis: - **Strength**: Existing software products and services providers - **Weaknesses**: Lack of unified certification schemes - **Opportunities**: Development of new schemes for certification taking into account the new EU certification framework - **Threats**: Unstable regulatory environment
Domain (JRC Taxonomy): Assurance, audit and certification
Sector (JRC Taxonomy): All sectors, with a focus on IT aspects of all these sectors.
Relation to Emerging Technologies: Artificial intelligence, Machine learning, Big data

Table 11: General information for Complex Dynamic Systems of Systems (from CAPE)

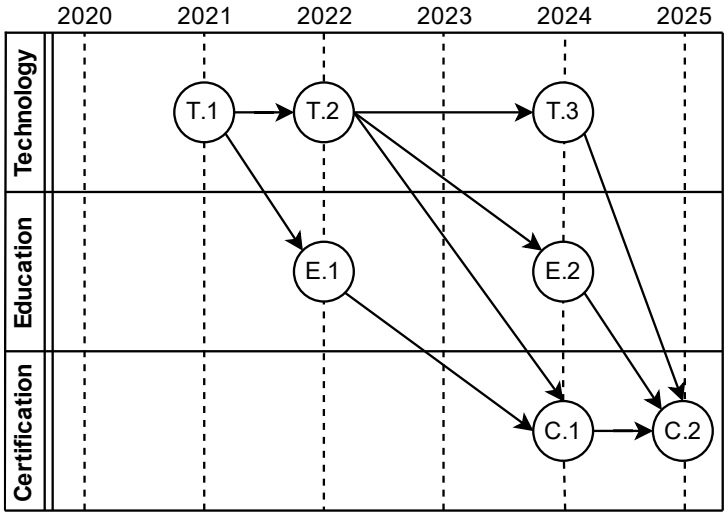


Figure 5: Timeline for expected completion of subgoals for Complex Dynamic Systems of Systems (from CAPE)

Stage/Dimension *Tx for Technology* *Ex for Education* *Cx for certification*	Sector (JRC)	Domain (JRC)	Regulation
T1	All sectors	Assurance, Audit and Certification	CC, SOG-IS
	Description (incl. obstacles): Decomposition of cybersecurity properties and description of cybersecurity property decomposition methodologies and tools **Description**: The objective of this technology is to facilitate the decomposition of security properties for complex systems, in so far as to be able to understand and verify individual properties. **Obstacles**: Decomposition of properties may lead to removing complex interactions, which will have an impact on global cybersecurity properties		
T2	All sectors	Assurance, Audit and Certification	CC, SOG-IS
	Description (incl. obstacles): Technologies for specifying time-varying properties and property combination methodologies and application to complex systems of systems **Description**: With the possibility to allocate resources and tailor decision based on demand and data, it becomes increasingly difficult to ensure that the needs for cybersecurity will be met by services all the time during execution. This is typically the case of denial of service attacks, where exceptional conditions defeat service execution. Assessment methodologies need to ensure that properties are met all the time, during the complete lifetime of a given system or service. **Obstacles**: Meeting cybersecurity requirements continuously may induce infeasibility or economic uncertainty. Assessment must include the capability to detect when certain properties cannot be met, either fully or due to constraints (economic, hardware, etc.) and provide methodologies for trade-off assessment and alerting of discarded properties.		
T3	All sectors	Assurance, Audit and Certification	CC, SOG-IS
	Description (incl. obstacles): Technologies for specifying time-varying properties driven by algorithms (e.g., AI, ML) and property combination methodologies for complex services **Description**: New AI-based technologies will induce needs for varying cybersecurity properties that must be verified at runtime and under		

	runtime conditions. This means that not only is the system dynamics, but the properties are dynamic as well. They may also vary according to dependencies between services that have a significant impact on property definition, negotiation and enforcement. Complex services relying on outside parties for service provisioning will need to define the properties that must be met by their third-parties providers, negotiate these properties in combination with the ones they need to guarantee to their customers, and verify that both their third parties meet their obligation and that they themselves meet the requirements of their customers. **Obstacles**: Assessment will be driven by economic and legal considerations (for example, economic efficiency of the service provider or the customer) and this must be reflected in the assessment.		
E1	All sectors	Assurance, Audit and Certification	CC, SOG-IS
	Description (incl. obstacles): Training and certification programs for evaluators of complex systems of systems		
E2	All sectors	Assurance, Audit and Certification	CC, SOG-IS
	Description (incl. obstacles): Training and certification programs for evaluators of complex services, including dynamic services driven by AI/ML techniques		
C1	All sectors	Assurance, Audit and Certification	CC, SOG-IS
	Description (incl. obstacles): Evaluation scheme for complex systems of systems **Obstacles**: Certification processes are heterogeneous in the EU and worldwide, leading to difficulties in globally certifying complex systems.		
C2	All sectors	Assurance, Audit and Certification	CC, SOG-IS
	Description (incl. obstacles): Evaluation scheme for complex dynamic services **Obstacles**: Certification processes are heterogeneous in the EU and worldwide, leading to difficulties in globally certifying complex services.		

Table 12: Detailed description of Complex Dynamic Systems of Systems (from CAPE)

6.3 HAII-T — High-Assurance Intelligent Infrastructure Toolkit

Title: High-Assurance Intelligent Infrastructures
Problem description: As small, connected devices evolve from being an Internet of Things (IoT) towards a true intelligent infrastructure (II), vulnerabilities in such devices become ever more critical.
Final goal: Secure-by-design development framework and toolkit supporting the design, development and verification of security-critical, large-scale distributed II systems.
Status Quo: - **Europe**: Multiple research institutes in Europe already research the security of the IoT (e.g., Secure IoT) - **International**: Multiple research institutes and international alliances focus already on research in the security of IoT (e.g., IoT Cybersecurity Alliance).
Estimated year of completion: 2025
Research aspect: Need to investigate possible threats to IIs, besides those affecting individual components; improve the security of OS and applications of IoT devices; provide orchestration framework supporting the security-by-design paradigm, including resilience and privacy protection.
Industrial demand: There is a huge market for IIs in a variety of domains, e.g., manufacturing, transportation, health & well-being, smart cities. While the industry devoted to the manufacturing of hardware and software components for individual components (sensors, actuators, networking) is thriving, the full potential of IIs will be achieved only through the provisioning of a secure-by-design development framework for large-scale II.
Social aspect: IoT technology is already threatening the users' privacy. As society will become more and more dependent on IIs, the availability of IIs is also bound to become a natural target for attackers. IIs are also likely to become a powerful attack vector (cf. Mirai attack). IIs will be widely accepted by society only if the security of their functioning will be ensured. Applied privacy-enhancing technologies as a part of a privacy-by-design framework will increase the trustworthy of IIs and IoT services and applications in society.
Benefit for EU: Virtually all industry sectors in the EU would gain a competitive edge with this technology, as it would enable them to offer secure products to the market. Additionally, the products will be natively in line with privacy regulations and standards.
SWOT Analysis - **Strengths**: Many EU research institutions are already working on the development of techniques that will contribute to the solution. - **Weaknesses**: Poor security in components. - **Opportunities**: Strengthening the industry by providing tools for the secure-by-design development of IIs. - **Threats**: Integration of different techniques is challenging. The computational complexity of privacy-enhancing technologies.
Domain (JRC Taxonomy): Security, Audit, and Certification; Cryptology, Data Security and Privacy; Identity and Access Management; Network and Distributed Systems; Software and

Hardware Security Engineering; Theoretical Foundations; Trust Management, Assurance and Accountability
Sector (JRC Taxonomy): Energy; Government and Public Authorities; Health; Maritime; Tourism; Transportation; Smart Ecosystem; Supply Chain; Public Safety
Relation to Emerging Technologies: IoT; Mobile devices; Edge Computing

Table 13: General information for High-Assurance Intelligent Infrastructures (from HAII-T)

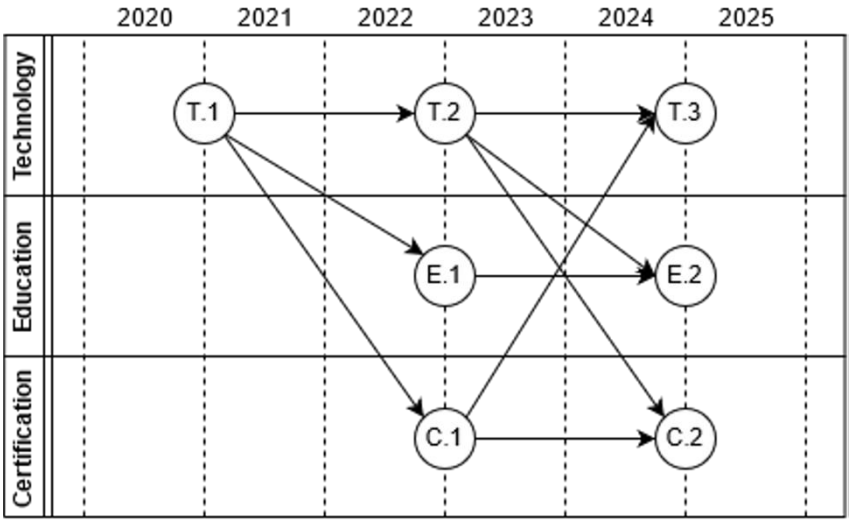


Figure 6: Timeline for expected completion of subgoals for High-Assurance Intelligent Infrastructures (from HAII-T)

Stage/Dimension *Tx for Technology* *Ex for Education* *Cx for certification*	Sector (JRC)	Domain (JRC)	Regulation
T1	Energy; Government and Public Authorities; Health; Transportation; Smart Ecosystem; Supply Chain; Public Safety	Security, Audit, and Certification; Cryptology, Data Security and Privacy; Identity and Access Management; Network and Distributed Systems; Software and Hardware Security Engineering; Theoretical Foundations; Trust Management, Assurance and Accountability	
	Description (incl. obstacles): HAII-T secure-by-design development framework and toolkit v.1 **Description:** The first version of HAII-T framework and toolkit will combine the first version of the techniques and technologies developed within HAII-T. Technologies will cover secure hardware, software and protocol verification, secure OS and more. **Obstacles:** The developed technologies deal with the security of the II at different levels, from hardware to software. Their integration in a unified framework is the major challenge.		
T2	Energy; Government and Public Authorities; Health; Transportation; Smart Ecosystem; Supply Chain; Public Safety	Security, Audit, and Certification; Cryptology, Data Security and Privacy; Identity and Access Management; Network and Distributed Systems; Software and Hardware Security Engineering; Theoretical Foundations; Trust Management, Assurance and Accountability	
	Description (incl. obstacles): HAII-T secure-by-design development framework and toolkit v.2 **Description:** The second version of HAII-T framework and toolkit will consist of an integration of the technologies that contributed to the first version. The integration will rely on a shared orchestration language. Moreover, the scalability of the technologies will be		

<table>
<tr><td></td><td colspan="3">demonstrated through selected use cases and benchmarks.

Obstacles: Scalability may be the major issue. As a matter of fact, purely theoretical approaches might fail to scale on large and complex systems such as those belonging to IIs.</td></tr>
<tr><td rowspan="2">T3</td><td>Energy; Government and Public Authorities; Health; Transportation; Smart Ecosystem; Supply Chain; Public Safety</td><td>Security, Audit, and Certification; Cryptology, Data Security and Privacy; Identity and Access Management; Network and Distributed Systems; Software and Hardware Security Engineering; Theoretical Foundations; Trust Management, Assurance and Accountability</td><td></td></tr>
<tr><td colspan="3">Description (incl. obstacles): HAII-T secure-by-design development framework and toolkit v.3

Description: The last version of the development framework and toolkit will be the final release. It will be used for the final project demonstration.

Obstacles: Beside the integration and scalability issues, the last version must also deal with usability requirements in order to be released to the public.</td></tr>
<tr><td rowspan="2">E1</td><td>Energy; Government and Public Authorities; Health; Transportation; Smart Ecosystem; Supply Chain; Public Safety</td><td>Security, Audit, and Certification; Cryptology, Data Security and Privacy; Identity and Access Management; Network and Distributed Systems; Software and Hardware Security Engineering; Theoretical Foundations; Trust Management, Assurance and Accountability</td><td></td></tr>
<tr><td colspan="3">Description (incl. obstacles): HAII-T training path for security-by-design of IIs (target: designers and developers of IIs)

Description: the training path will include the presentation and training material for the technologies and techniques involved in the toolkit and contributing to the security-by-design development process.</td></tr>
</table>

	Obstacles: Each technique/technology may have a different level of maturity and the training path could be inhomogeneous.		
E2	Energy; Government and Public Authorities; Health; Transportation; Smart Ecosystem; Supply Chain; Public Safety	Security, Audit, and Certification; Cryptology, Data Security and Privacy; Identity and Access Management; Network and Distributed Systems; Software and Hardware Security Engineering; Theoretical Foundations; Trust Management, Assurance and Accountability	
	Description (incl. obstacles): HAII-T training path for security-by-design of IIs (target audience: scientists and engineers interested in the development and extension of the HAII-T framework) **Description:** The HAII-T framework will be designed to be extensible. Domain experts will be trained to understand the framework structure, functionalities and logic. In particular, they will learn how to plug new techniques in the framework. **Obstacles:** Some techniques may be very domain specific and the integration may not be guaranteed. This will be assessed through concrete examples.		
C1	Energy; Government and Public Authorities; Health; Transportation; Smart Ecosystem; Supply Chain; Public Safety	Security, Audit, and Certification; Cryptology, Data Security and Privacy; Identity and Access Management; Network and Distributed Systems; Software and Hardware Security Engineering; Theoretical Foundations; Trust Management, Assurance and Accountability	
	Description (incl. obstacles): HAII-T light-weight security certification framework for IIs **Description:** The certification framework will provide system designers with a set of security properties that have been verified on the II blueprint **Obstacles:** The light-weight certification might not apply to the actual II, but only to the blueprint. Also, the correlation with existing		

	certification frameworks may be not granted.		
C2	Energy; Government and Public Authorities; Health; Transportation; Smart Ecosystem; Supply Chain; Public Safety	Security, Audit, and Certification; Cryptology, Data Security and Privacy; Identity and Access Management; Network and Distributed Systems; Software and Hardware Security Engineering; Theoretical Foundations; Trust Management, Assurance and Accountability	
	Description (incl. obstacles): HAII-T (full-fledge) security certification framework for IIs **Description:** The certification framework will provide the designers with a rich and detailed list of certified properties. Each of them will apply to a specific stage of the II development process (e.g., design vs. testing). The certification framework will also highlight correspondence between the certified properties and the existing legal frameworks. **Obstacles:** The correspondence between the certification and the legal frameworks might be partial.		

Table 14: Detailed description of High-Assurance Intelligent Infrastructures (from HAII-T)

6.4 SAFAIR — Secure and Fair AI Systems for the Citizen

Title: Secure and Fair AI Systems for Citizen

Problem description: The proliferation of Artificial Intelligence systems in contemporary lifestyle brings about both astonishing benefits and brand-new challenges for society. While the gains and the prosperity delivered by AI are abundant in all walks of life, starting from most obvious ones, like image recognition, search engines, recommender systems, autonomous systems, including vehicles, to less obvious uses, like cybersecurity. The widespread adoption of AI does not consider that those algorithms were developed not taking into account the adversarial nature of real-life implementations. Thus, an array of problems emerges. First and foremost, the bulk of above-mentioned algorithms have a black box nature. This means that even though the insights provided those methods are meaningful and valuable, no one can easily explain how exactly the AI came to its conclusions. Every machine learning model, prior to applying it, has to be trained. The training can be run in any of the following three ways: supervised, unsupervised and semi-supervised. Each of them has its advantages and drawbacks and is used in different applications. While the ML algorithms invariantly fit the presented data, it is a challenging task to try to explain how specific data affects certain aspects of the algorithms, which then translates to the end result. One of the facets of the SAFAIR program attempts to address the situation by enhancing the explainability of AI. Secondly, methods exist that allow to compromise AI itself in several ways. A knowledgeable adversary can influence the way an AI classifier judges a specific data point, thus evading detection. A malicious user could also provide a series of inputs in the training, or re-training phase of a classifier – in other words poison the data – to make the algorithm behave in a way that is beneficial to the adversary. Thirdly, a trained AI setup constitutes a major expenditure of expert time and therefore company resources. This makes an AI model a valuable intellectual property. There are ways, however, to fit one classifier to the output of another classifier, essentially stealing the original algorithm. Last, but not least, any bias on the AI part, especially in socially sensitive areas, could relatively easily seed distrust to AI technology among the general public. In the midst of all that, there are new cybersecurity challenges that gain ground recently. With the universal danger of cybersecurity breaches, enhancing the cybersecurity condition and detection algorithms is of absolute importance. Malware is now identified as the stern menace for commercial and critical IT systems, as well as for the general public. Malware, however, is adequately comprehended and can be dealt with sensibly well. A more menacing challenge arises, stegomalware and the use of the information hiding techniques by cyber-criminals.

In the near-future, one of the challenges of both AI and Cybersecurity will be to propose, implement and validate innovative AI/ML-based solutions to analyse network traffic, binary code, and applications in order to detect novel types of malware including crypto-malware.
One of the intrinsic aspects of malware detection is that it is an arms race, where the adversaries are constantly developing new ways to circumvent the security measures.
In this arms race, novel and emerging technologies are employed by both sides of the conflict. The analysis of crypto malware and encrypted traffic potentially generated by malware samples is an emerging research topic, driven by the increase of this kind of malware. The fast adaptation of those techniques by the malicious actors and the lack of adequate response to this threat is expressed by the fact that a very limited number of scientific papers have been published on the topic, even though current malware analysis, detection techniques and tools are mostly not mature enough and ready to cope with this new trend. Current research in this area (study of cryptography deployment in malware) maps the usage of cryptographic primitives among the malware authors, not describing the ecosystem as a whole. In addition, there are ad hoc searches for weaknesses in malware implementations of cryptography that aim to block the function of the malware. Systematic and thorough analyses in this area are required and seem like a natural step where AI/ML methods can definitely play a crucial role.

The most effective, state-of-the-art AI algorithms are also notorious for being opaque, black-box models. They are capable of providing highly accurate results, but do not augment the results with any understanding to impart to the security operatives. In the future, the researchers will not only continue to push the development on finding ways to make AI algorithms more adequate in the actual deployment, but also will work on explainability and security of AI methods themselves, providing methods for enhanced understanding and better resilience of AI models.
Currently, research into explainable AI (xAI) is mostly concerned with developing new methods and tools. However, there are no metrics to reliably measure the effectiveness of xAI and whether the explanations provided are helpful or even if they are true. In addition to investigating new approaches of xAI to augment and supplement the tools and methods found at the cutting edge of AI research, the researchers need to formulate appropriate metrics for expressing the effectiveness of AI explainability methods in the applied context.
New AI paradigms open up new possibilities, yet new paradigms expose new attack vectors as well. Federated learning distributes the training of a model to local machines, and each of those machines maintains a local training subset of data, only uploading the aggregate model to the server. A local training subset of data makes a data poisoning attack a much more viable vector than in traditional ML approaches - in case of the compromise of one of the local machines.

Another challenge concerns the future ML model markets and MLaaS schemas. There is a need for research on methods and techniques that ensure protection of the models in the face of threats related to transferability of AI as part of the Secure AI challenge. For instance, transfer learning can be used to erase watermarks introduced in the model to protect model IPR. Means and mechanisms to tackle this kind of issues are fundamental to enable an EU Digital market.

Final goal:

- Enhanced explainability of AI systems
- More reliable and resilient AI systems
- Better threat understanding in AI context including the use of AI for malicious activities
- More effective methods and tools for analysis of security threats for AI systems
- A set of techniques and solutions for AI systems protection
- Systems in place to ensure fairness of AI systems
- Defensive and reactive mechanisms geared towards novel cybersecurity threats
- Cybersecurity systems being able to detect stegomalware

Status Quo:

- **Europe:** Preliminary research on adversarial techniques has been conducted in several research institutions in Europe, as well as work on explainability of AI
- **International:** DARPA programs

Estimated year of completion: 2022 (program) / 2026 (possible extensions)

Research aspect: Contemporary threats to AI systems need to be investigated, and suitable countermeasures need to be developed. An in-depth analysis of current adversarial threats needs to be performed. As the threats evolve, the ability to address the needs to keep up. With no adequate measures for AI explainability, AI fairness and most importantly AI security, all of those aspects require suitable analysis. Defensive and preventive mechanisms need to be established. Along with improving the robustness of AI itself, research on new cybersecurity threats, like information hiding and ransomware is in demand. The research in the domain of AI will evolve to cover new grounds and answer new questions, like how to effectively measure the veracity and relevance of explanations provided by novel xAI methods, Novel attack vectors are going to be open with new paradigms of AI, and adequate precautions will need to be

researched and implemented. Most notably, federated learning might be a new open door for the proliferation of data poisoning attacks. On the flip side, AI could provide the answer to new threats, like crypto-malware.
Industrial demand: Every industry relying on AI technology is now vulnerable to adversarial attacks; this includes critical, sensitive domains, like automotive, government, medical fields, security-related, etc. Providing secure and explainable AI systems would increase trust in these kinds of systems, allowing further adoption, and preventing possible adversarial intrusions, hijacking of algorithms, or breakdowns. Risks are related to the various classes of assets. Structures like payment systems in the financial arena, embedded systems, cloud computing services and systems processing personal data are especially exposed to the danger of cyberattacks.
Social aspect: The wide audience needs to trust AI solutions to rely on the decisions inferred from data. The possibility of manipulation of AI breaks this trust and makes the whole big data ecosystem unreliable. Thus, AI resilient to adversaries is necessary. Appropriate use and re-use of data are mandatory for AI systems to continue to flourish. Thus, setting up systems to make AI compliant with current and upcoming data-related legislation is of utmost importance. Furthermore, establishing a track record of what is perceived by the general public as fairness with regards to how AI operates has the potential of accumulating trust to those kinds of solutions.
Benefit for EU: This kind of technology could provide EU AI industry a leading position on the global market, given the unique selling proposition of the only secure AI on the market
SWOT Analysis: - **Strengths**: Some of the finest EU research institutions are working to resolve the problem - **Weaknesses:** The need is pressing but the solutions require time - **Opportunities:** The acquisition of necessary knowledge might be good grounds for the training of the high tier scientific personnel - **Threats**: The solution might be overly complicated computationally to be applicable in cybersecurity – where computational overhead is already a valuable metric for the applicability of ML algorithms
Domain (JRC Taxonomy): Theoretical Foundations, Human Aspects, Legal Aspects, Data Security
Sector (JRC Taxonomy): Health, Energy, Financial, Government, etc.
Relation to Emerging Technologies: Artificial Intelligence, Big Data, Autonomous Machinery, Robotics, Threat Intelligence

Table 15: General information for Secure and Fair AI Systems for Citizen (from SAFAIR)

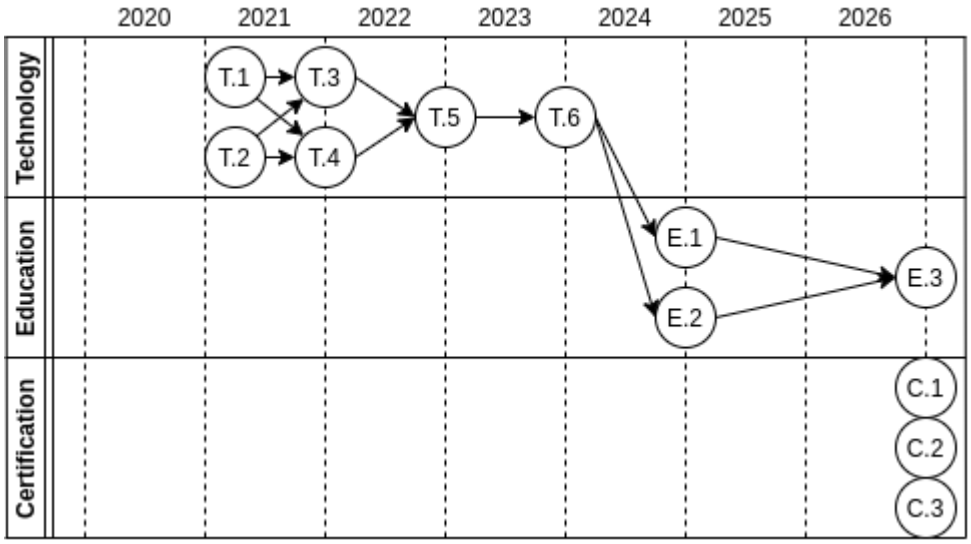


Figure 7: Timeline for expected completion of subgoals for Secure and Fair AI Systems for Citizen (from SAFAIR)

Stage/Dimension *Tx for Technology* *Ex for Education* *Cx for certification*	**Sector (JRC)**	**Domain (JRC)**	**Regulation**
T1	All sectors	Cybersecurity	Guidelines for Trustworthy AI.
	Description (incl. obstacles): The comprehensive AI threat analysis, including threat mechanisms, novel threats in cybersecurity and AI, and description of necessary tools		
T2	All sectors	Cybersecurity	Guidelines for Trustworthy AI.
	Description (incl. obstacles): A preliminary description of the security systems for AI, including defensive and reactive measures, enhanced explainability of AI and improved measures for fairness		
T3	All sectors	Cybersecurity	Guidelines for Trustworthy AI.
	Description (incl. obstacles): A plan for the verification and evaluation for the testing phase of the SAFAIR program		

T4	All sectors	Cybersecurity	Guidelines for Trustworthy AI.
	Description (incl. obstacles): The first demonstration of the mechanisms and tools for securing Artificial Intelligence-based systems		
T5	All sectors	Cybersecurity	Guidelines for Trustworthy AI.
	Description (incl. obstacles): The final version of security mechanisms and tools for AI systems		
T6	All sectors	Cybersecurity	Guidelines for Trustworthy AI.
	Description (incl. obstacles): Knowledge, experience and methods addressing threats related to AI transferability and AI reuse across applications and sectors, e.g. addressing model stealing and IPR issues. Obstacles to achieve the task include the need of datasets from different context/applications/sectors that enable testing and understanding AI transferability threats and potential remediations.		
E1	All sectors	Theoretical Foundation, Human Aspects, Data Security	
	Description (incl. obstacles): The SAFAIR secure AI educational program, explaining the threats of adversarial learning along with the defensive and reactive measures		
E2	All sectors	Theoretical Foundation, Human Aspects, Data Security	
	Description (incl. obstacles): The SAFAIR fair AI educational program, explaining the possible ways bias could twist the decisions of AI and the ways to prevent that from happening		
E3	All sectors	Theoretical Foundation, Human Aspects, Data Security	

	Description (incl. obstacles): The SAFAIR explainable AI educational program, walking the individuals, start to finish, through the necessary knowledge and skills to deploy successful, secure, fair and explainable AI solutions in a way that is agnostic to the domain		
C1	All sectors	Theoretical Foundation, Human Aspects, Data Security	
	Description (incl. obstacles): A certification exam for ICT professionals proving their ability to secure AI algorithms against adversarial threats, checking the individual's ability to understand, spot, secure against, react to and eliminate the threat of adversarial attacks on machine learning algorithms		
C2	All sectors	Theoretical Foundation, Human Aspects, Data Security	
	Description (incl. obstacles): A certification exam for ICT professionals proving their ability to secure AI algorithms against any possible bias either coming from data collection or from the way the specific algorithms process the data		
C3	All sectors	Data Security	
	Description (incl. obstacles): THE SAFAIR SEAL OF APPROVAL - A certification geared towards the venues utilizing AI, proving the utilized algorithms are secure, explainable and fair.		

Table 16: Detailed description of Secure and Fair AI Systems for Citizen (from SAFAIR)

Chapter 7 Transversal Challenges

This chapter describes work packages WP9 and WP11, covering “cybersecurity training and awareness” and “certification organization and support”. These challenges are also based on the SPARTA Working Packages, but also give a broader picture of goals that the WP Leaders found important for the EU.

7.1 Education and Training

Title: Education and Training in Cybersecurity
Problem description: Individual academic and professional programs are already available at many universities and training institutions, but there is a lack of coordination and understanding, what courses and topics should be included in these programs so that they reflect the current trends on the job market.
Final goal: Provide best-practice curricula for both universities and training institutions reflecting skills necessary for a wide spectrum of roles in cybersecurity. Rollout the programs at a substantial number of universities.
Status Quo: - **Europe:** Sample curricula are not yet available on the European level, though ENISA began works on these tasks. Some universities provide their individual programs, as well as professional training institutions. - **International:** Mainly USA provide recommendations on creating cybersecurity study programs. Mainly ACM (Association for Computing Machinery) and DHS (Dpt. Of Homeland Security) with NSA (National Security Agency) provide sample curricula and programs.
Estimated year of completion: 2024
Research aspect: Existing study programs, courses and training need to be identified. Skill matrix (skill x role mapping) needs to be established. Topics for courses need to be identified and collected to the curricula. New methods of teaching and training, especially the hands-on training activities, need to be developed and tested.
Industrial demand: The demand for cybersecurity experts is extraordinary internationally, both at companies and in the public sector.
Social aspect: By providing top-quality education in security, graduates get high-qualification jobs more easily and employees can reach to higher positions in their respective jobs.
Benefit for EU: Better competence in cybersecurity, more secure ICT environment, better

protection against external threats, and the more balanced situation on the job market.
SWOT Analysis: - **Strengths:** Good experience in the consortium, some programs already rolled out, good practice from non-EU countries. - **Weaknesses:** Not all roles on the job market can be reflected in the first best-practice curricula, curricula need to be finalized and individualized by universities and training institutions. - **Opportunities:** No EU-level best practices for education exist now, strong demand in the job market for experts in cybersecurity. - **Threats:** Curricula are not widely accepted by institutions, new programs are not accepted at national levels (e.g., due to accreditation processes)
Domain (JRC Taxonomy): Cybersecurity Education, Cybersecurity Exercises, Cyber Ranges, Certification Programmes, Cybersecurity Education Methodology.
Sector (JRC Taxonomy): Government and Public Authorities, Publishing, Internet
Relation to Emerging Technologies: Cyber Ranges, Gamification

Table 17: General information for Education and Training in Cybersecurity

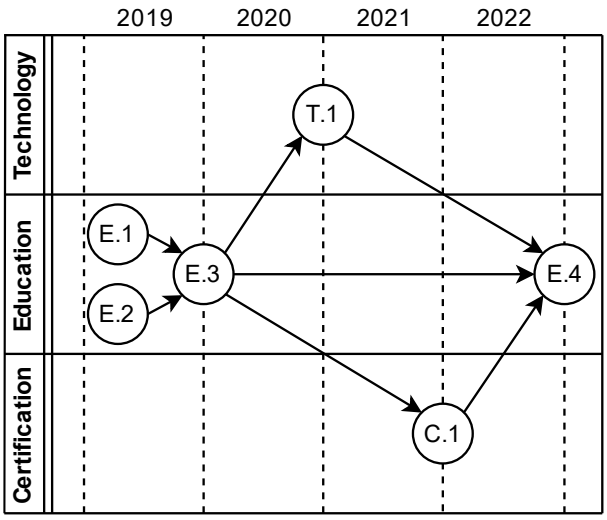


Figure 8: Timeline for expected completion of subgoals for Education and Training in Cybersecurity

Stage/Dimension *Tx for Technology* *Ex for Education* *Cx for certification*	**Sector (JRC)**	**Domain (JRC)**	**Regulation**
T1	Equivalent to Table 17	Cybersecurity Education, Cybersecurity Exercises, Cyber Ranges	
	Description (incl. obstacles): Design and implementation of cyber ranges and cooperation training platforms		
E1	Equivalent to Table 17	Cybersecurity Education	
	Description (incl. obstacles): Creation of a skill matrix (role x skill mapping)		
E2	Equivalent to Table 17	Cybersecurity Education, Cybersecurity Education Methodology	
	Description (incl. obstacles): Analysis of current programs and courses		
E3	Equivalent to Table 17	Cybersecurity education, Cybersecurity education methodology	
	Description (incl. obstacles): Development of best practice curricula		
E4	Government and Public Authorities	Cybersecurity education	

	Description (incl. obstacles): Pilots with real students		
C1	Government and Public Authorities	Cybersecurity education, Cybersecurity education methodology, Certification Programmes	National accreditation processes
	Description (incl. obstacles): Implementation of best-practice curricula into a study program, including accreditation and certification (where possible)		

Table 18: Detailed description of Education and Training in Cybersecurity

7.2 Certification Organization and Support

Title: Certification Organization and Support - Mapping of international and European cybersecurity certification

Problem description: Given the growing threats that connected systems face, it has become important to protect IT-based infrastructures and systems sufficiently. Cybersecurity certification is one way to help engineers design more secure systems. Over the years, many cybersecurity standards and certifications schemes have been created at both European and international level. In the context of the European Digital Single Market, it is important to have a simple cybersecurity certification scheme that is recognized throughout all European countries. To move in this direction there is a need to analyse different national European cybersecurity initiatives as well as international efforts in order to identify commonalities and differences. Standards and certification schemes can be classified in different ways. Some standards and schemes have been designed for products and others for processes and services. Other standards are sector-specific such as in transport or aeronautics. Others focus on specific technologies, e.g., networks or cloud computing. More widespread adoption of cybersecurity certification in the design of connected products and services will be successful only if certification is perceived as cost-effective and that it effectively improves the quality of products and services. For certification to be more widely adopted in security engineering, there is a clear need to design more agile certification processes, to better integrate certification in the security engineering process, and to improve the effectiveness of certification schemes. Certification of AI systems which poses a major challenge unless assurance of fairness and explainability of AI systems is not yet solved. In fully distributed and Cloud based service architectures, where not only Cloud providers but also Cloud resource configuration may evolve rapidly, the certification of services that use hardware and software from multiple third parties in the value-chain is a task for which research is still needed. Automation of certification is also a long-term challenge towards which the certification market should start adapting. Furthermore, in a globalized market it is necessary that the European certification schemes in the Digital Single Market are clearly mapped to other international certifications with which they would need to coexist, providing a clear added value with respect to them.

Final goal: Identification of commonalities and differences between national cybersecurity certification initiatives and recommendations for convergence at the European level.

Status Quo:

- **Europe:** Several European countries have taken initiatives in terms of cybersecurity certification. One of the objectives of the recent EU cybersecurity act is to create a European cybersecurity framework. This will lead to the creation of EU wide certification schemes that will require convergence and consensus among EU member states.
- **International:** There are many existing international cybersecurity standards for products, processes and services as well as many sector-specific, e.g., railway or automotive, or technology, e.g., IoT, specific standards.

Estimated year of completion: 2022

Research aspect: Cybersecurity certification schemes can be complex and costly to apply and may not always provide the expected improvement in the level of protection. It is thus important to carry out research to understand how to design more agile and flexible certification processes

that provide improvements in the level of protection.
Industrial demand: The EU cybersecurity certification framework will be voluntary and not mandatory. It will be up to sectorial certification schemes, e.g., for critical infrastructure and 5G, to define whether certification is mandatory or not.
Social aspect: Clients of systems are becoming worried about cybersecurity threats and are asking that systems be more thoroughly tested for cybersecurity. This is particularly true for industrial systems in critical infrastructure with strong safety requirements.
Benefit for EU: European systems and services that are well protected will contribute to the image of quality for European products and services.
SWOT Analysis: - **Strengths:** Cybersecurity certification is a topic of interest for all European countries due to the NIST Directive - **Weaknesses**: There is a lot of divergence currently between member state approaches - **Opportunities:** The EU Cybersecurity Act is an opportunity to make national and international cybersecurity certification schemes converge more**.** - **Threats:** Pushing for more cybersecurity certification can be costly and could have an impact on the competitiveness of European products and services.
Domain (JRC Taxonomy): Assurance, audit and certification
Sector (JRC Taxonomy): All sectors
Relation to Emerging Technologies: Threat Intelligence. Artificial intelligence can be used to attack and to protect systems from attack.
Contribution to the EU strategic autonomy: The SPARTA certification roadmap is in line with European strategic objectives in terms of cybersecurity certification. The EU Cybersecurity Act includes the definition of a European cybersecurity certification framework. “The purpose of the EU cybersecurity certification framework under the Regulation (EU) 2019/881 is to establish and maintain the trust and security on cybersecurity products, services and processes” (https://www.enisa.europa.eu/topics/standards/certification). The SPARTA WP11/T11.1 roadmap will contribute by analysing and comparing some existing and emerging cybersecurity standards and making recommendations on how to apply them in a more agile and effective manner.

Table 19: General information for Certification Organization and Support

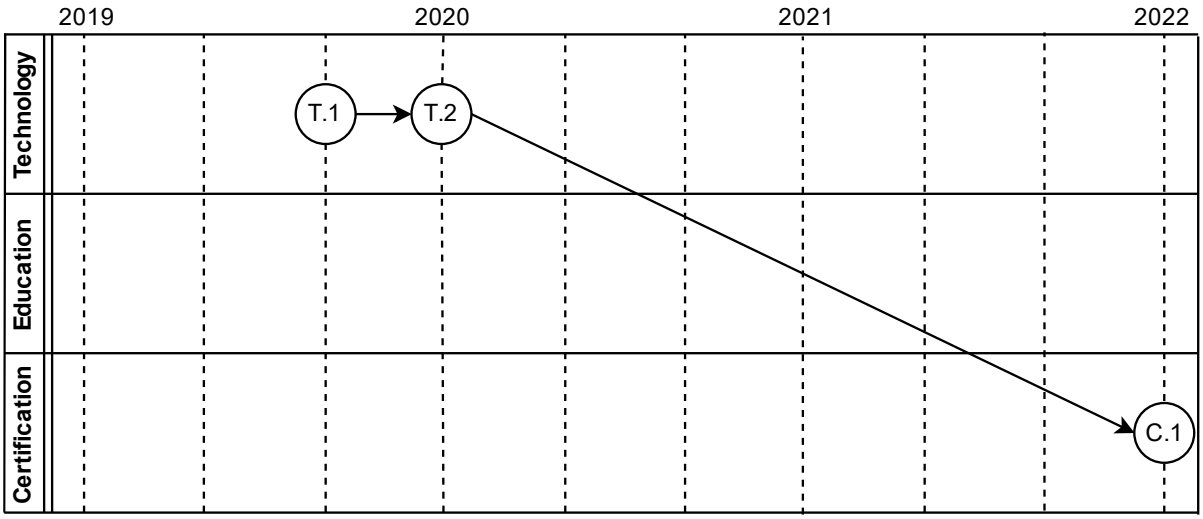


Figure 9: Timeline for expected completion of subgoals for Certification Organization and Support

Stage/Dimension *Tx for Technology* *Ex for Education* *Cx for certification*	**Sector (JRC)**	**Domain (JRC)**	**Regulation**
T1	Transportation, Financial, Government and Public Authorities	Data Security and Privacy; Assurance, Audit and Certification	
	Description (incl. obstacles): Identify and compare existing cybersecurity standards and certification schemes. We will select one or several standards and compare them to understand their commonalities and differences. We could take for example the area of SME cybersecurity certification where several European countries have taken initiatives. By comparing them, we could make recommendations towards a European SME cybersecurity scheme.		
T2	Transportation, Financial, Government and Public Authorities	Data Security and Privacy; Assurance, Audit and Certification	
	Description (incl. obstacles): Identify requirements on assessment tools and processes. In order to make cybersecurity certification		

C1	Transportation, Financial, Government and Public Authorities	Data Security and Privacy; Assurance, Audit and Certification	
	Description (incl. obstacles): Provide recommendations on certification based feedback from the assessment tools developed in the CAPE research program.		

Table 20: Detailed description of Certification Organization and Support

Chapter 8 Emerging Challenges

This chapter covers new emerging challenges that were identified during the SPARTA roadmapping activities.

8.1 User-Centric Data Governance

Title: User-Centric Data Governance
Problem description: Our connected world experiences unprecedented growth in terms of personal, increasingly intrusive data collection, be it while surfing the web, using a smartphone, or driving a connected car. At the same time, data protection regulation has evolved in Europe with the General Data Protection Regulation (GDPR) that came into effect on May 2018 to better protect the European Union resident in this connected world. These evolutions raise three general types of questions. Certain questions are related to the privacy principles that need to be better understood and defined. For example, what is a proper notion of user control, and what are the proper ways of providing the user with empowerment and privacy information? Tools are also needed in several domains of privacy. For instance, the GDPR provides little guidance about the effective implementation of some of the concepts it puts forward, like Data Protection Impact Assessments (DPIA). More generally, and independently of GDPR, a broad set of Privacy Enhancement Tools (PET) are required, from database anonymization technics (e.g., required by open-data initiatives) to various forms of privacy-preserving protocols (e.g., for unlinkability or anonymized communications). Finally, the lack of transparency in our connected world, with many services and devices behaving as black boxes, and the lack of user control, are major issues. How to express consent or opposition in the absence of information or user interface? Identification of such hidden behaviours, which requires data flow analyses, is hindered by the number, complexity, and diversity of underlying applications and communication technologies. Challenging transverse research activities are required to bring transparency, highlight good and bad practices, and enable regulators to enforce data protection laws.
Final goal: The goal of any activity in privacy is to give the ability for individuals to control their personal data and decide what to reveal, to whom, and under what condition. To this end, several dimensions need to be considered: at the principle and regulation level, at the PET level, and in existing systems of our connected world.
Status Quo: - **European Union:** To consider the major changes that took place during the last decade in terms of collection and use of personal data, the European Union adopted the General Data Protection Regulation (“GDPR”) that came into effect on May 2018. The main change is the emphasis put on the responsibility of the data controllers, i.e., the organizations processing personal data, as well as their sub-contractors if there are any. Any data controller must conduct data protection impact assessments, implement privacy

by design and be accountable. If the impact assessment indicates that the processing is likely to severely impact the rights and freedoms of physical persons, the measures taken will have to be strengthened. The rights of data subjects are also strengthened with better information and control over their data, following the user empowerment philosophy.

- **International:** The application of the European GDPR and its significant sanctioning power has focused a lot of interest on data protection. Several countries may progressively follow the European Union example and make their data protection laws more protective for their citizens. On the other hand, the GDPR comes into conflict with the data protection laws of several non-European countries, the USA being one of them. International agreements have been signed (in this particular case, the Privacy Shield) in order to clarify the legal responsibilities of US companies. However, the adoption of the Clarifying Lawful Overseas Use of Data Act (A.K.A. Cloud Act) mid-2018 by the USA, facilitates the access to data by the police and surveillance authorities, no matter the server location, in the USA or elsewhere. Cultural differences between European countries also account for differences in the respective laws, including for such a fundamental definition as that of Personal Data.

Estimated year of completion: 2030.

Research aspect:

We can define several categories of research activities:

- **Privacy protection technologies and tools:**
  Privacy protection requires the setup and the use of a large number of technologies and tools (or PET, Privacy Enhancement Technologies). Some of these technologies are approaching maturity, while others (e.g., homomorphic encryption) remain so challenging that availability forecasts are almost impossible. Finally, certain technologies (e.g., anti-tracking tools for web browsing) are subject to constant evolutions, as web tracking techniques becomes more sophisticated.
  Examples of such technologies and tools include Attribute-Based Credentials, Blind signatures, Homomorphic encryption, PETs in Access Control, Privacy by standard cryptography, Pseudonymous systems, Proof of knowledge protocols, Secret sharing, Secure multi-party computation, Anonymizing networks, Anti-tracking tools, Onion routing, Data aggregation, Data acquisitions/collection, Database privacy, Data swapping, Generalization, Microdata protection, Obfuscation-based privacy, or Web privacy (anti-tracking technologies);

- **Analysis of privacy threats and attacks:**
  As in cryptography, where cryptanalysis (i.e., deliberate attacks) play a key role in assessing the security of cryptographic components, several PETs (see T.1) must be challenged by privacy researchers. For instance, de-anonymization attacks are key to assess the efficiency of database anonymization and thereby in bringing confidence in the related anonymization technologies.
  This category of activity also involves the practical analysis of several ecosystems, IoT or smart buildings being two examples. Many questions arise like what are the actors? What are the practices? What data is collected and to whom is it sent? What is the underlying economic model?
  Challenges include: Generic attacks to privacy, Location tracking, Malware based on privacy leakages, Data correlation, Data profiling, Information leakage, Location leakage, Side channels, Differential privacy,
  k-Anonymity concepts, or measuring and quantifying privacy;

- **Privacy Evaluation:**
  Formal methods can play a key role in privacy evaluations of systems and services. For

instance, it can be key in assessing architectures and being in a position to prove compliance with regulation, or to reason and assess the adequacy of privacy policies, or in performing Data Protection Impact Assessment.
Research in this area includes Model definitions, Policy languages and tools for privacy, Data Protection Impact Assessment tools, Evaluation of PETs in systems, or Audits;

- **Privacy-preserving management and regulations:**
Regulation plays a key role in personal data protection. However, the regulation defines generic concepts (e.g., a user control) that often need to be further defined, taking into account various dimensions (e.g., technical, human, legal, economic). The regulation also requires a data controller to perform privacy risks analysis, or be accountable for his actions, which further raises additional questions (e.g., keeping records of actions performed without creating additional privacy risks). Other aspects, like usability, control, consent, or information, also play a key role in the privacy landscape.
The relevant topics in this category includes: Concept and design strategies, Human factors, usability and user-centered design for PETs, Personal data life cycle, PETs controls matrix, Privacy by design, Privacy principles of ISO/IEC 29100, Consent mechanisms, Compliance with regulations, Legal regulations, National laws related to privacy in EU and rest of World, or Privacy policy enforcement.

Industrial demand:

- Any business has to conform to the GDPR. Understanding the concepts, having at our disposal practical tools, having open, accountable, secure and private-by-design procedures are mandatory.
- Beyond the legal aspect, it is the long-term interest of private companies to improve their relationships with their clients. Improving trust in the products and services that are provided is key for sustainable relationships, in a context of massive data collection. Bringing transparency, accountability and control to the end-users are key aspects.

Social aspect:

- The user trust in the digital, connected world is key to its acceptance. Without trust, digital evolution runs the risk of being subject to a major rejection.
- End-users are often inclined to declare themselves concerned by privacy while at the same time behaving in an opposite manner. This well-known “privacy paradox” highlights the need for sociological studies to better understand human behaviours in this domain and potentially improve awareness and practices.

Benefit for EU:

- Promote the European values relative to digital rights, and thus promote the European model of data protection.
- Enhance the European offer in terms of Privacy Enhancement Tools.
- Continue to be an international leader in terms of data protection.
- Favour the success of companies that promote privacy as a key differentiator with respect to non-European competitors.

SWOT Analysis:

- **Strengths**: Privacy is a highly accepted European value both by politicians and by citizens, and is supported by high-level academic research.
- **Weaknesses:** Industrial leaders in digital services seat in the US and in China and are continuously collecting huge amounts of personal data of European citizens and

residents. - **Opportunities**: The GDPR implementation and the increase awareness of threats against privacy. - **Threats**: Privacy may have to face conflicting concerns. There is a fundamental tension between privacy and surveillance, but also privacy and utility (e.g., during database anonymization).
Domain (JRC Taxonomy): Data security and privacy
Sector (JRC Taxonomy): Potentially all (perhaps except nuclear)
Relation to Emerging Technologies: With the advent of IoT, privacy leaks may reach an unprecedented level in volume and precision, both within the digital and physical worlds, and often without the user's knowledge.

Table 21: General information for User-Centric Data Governance

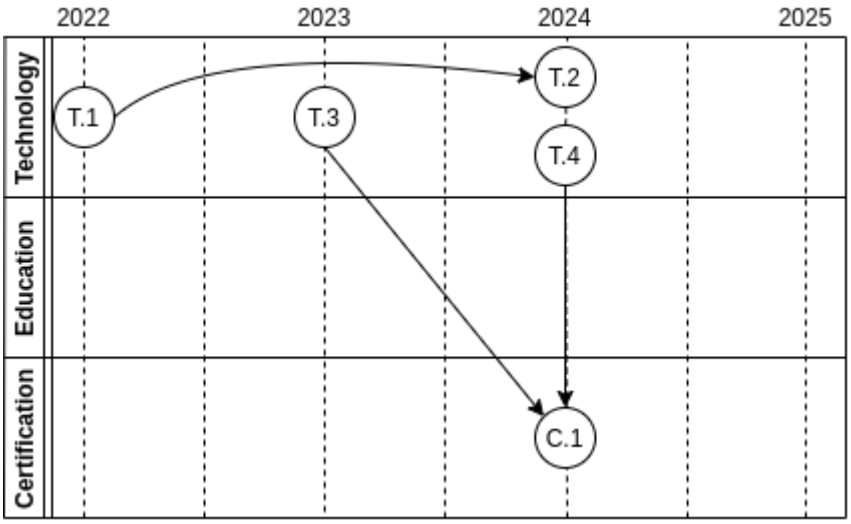


Figure 10: Timeline for expected completion of subgoals for User-Centric Data Governance

Stage/Dimension *Tx for Technology* *Ex for Education* *Cx for certification*	**Sector (JRC)**	**Domain (JRC)**	**Regulation**
T1	Transversal to all sectors	Equivalent to Table 21	
	Description (incl. obstacles): Privacy protection technologies and tools. Activities include: Attribute-Based Credentials, Blind Signatures, Homomorphic Encryption, PETs in Access Control, Privacy by Standard Cryptography, Pseudonymous Systems, Proof of Knowledge Protocols, Secret Sharing, Secure Multi-Party Computation, Anonymizing Networks, Anti-Tracking Tools, Onion Routing, Data Aggregation, Data Acquisitions/Collection, Database Privacy, Data Swapping, Generalization, Microdata Protection, Obfuscation-Based Privacy, or Web Privacy (Anti-Tracking Technologies).		
T2	Smart ecosystems, Transportation, Health, Digital infrastructure	Equivalent to Table 21	
	Description (incl. obstacles): Analysis of privacy threats and attacks. Activities include: Generic attacks to privacy, Location tracking, Malware based on privacy leakages, Data correlation, Data profiling, Information leakage, Location leakage, Side channels, Differential privacy, k-Anonymity concepts, or Measuring and quantifying privacy.		
T3	Smart ecosystems, Transportation, Health, Digital infrastructure	Equivalent to Table 21	
	Description (incl. obstacles): Privacy Evaluation. Activities include: Model definitions, Policy languages and tools for privacy, Data Protection Impact Assessment tools, Evaluation of PETs in systems, or Audits.		
T4	Equivalent to Table 21	Assurance, Audit, and Certification; Data Security and Privacy;	

		Legal Aspects; Trust Management, Assurance, and Accountability.	
	Description (incl. obstacles): Privacy-preserving management and regulations. Activities include: Concept and design strategies, Human factors, usability and user-centered design for PETs, Personal data life cycle, PETs controls matrix, Privacy by design, Privacy principles of ISO/IEC 29100, Consent mechanisms, Compliance with regulations, Legal regulations, National laws related to privacy in EU and rest of World, or Privacy policy enforcement.		
C1	Equivalent to Table 21	Assurance, Audit, and Certification; Data Security and Privacy; Legal Aspects; Trust Management, Assurance, and Accountability.	
	Description (incl. obstacles): Evaluation / certification of privacy in applications and systems. With the enforcement of the GDPR and soon ePrivacy regulations, the European landscape in terms of data protection has witnessed major evolutions. New obligations (e.g., conducting a DPIA) now apply to Data Controllers. This trend will further continue, as it is the case with cybersecurity at the European level.		

Table 22: Detailed description of User-Centric Data Governance

8.2 Autonomous Security for Self-Protected Systems

Title: Autonomous Security for Self-Protected Systems

Problem description: With the constant and significant increase in the speed with which attacks spread or are able to spread, it has become crucial on the one hand to be able to detect these attacks in real-time, and on the other hand to be able to diagnose these attacks in order to consider *in fine* the automatic implementation of countermeasures.

Final goal: Following the idea of autonomous computing, this challenge ultimately aimed to develop a computer system capable of self-managing its own security. The goal is thus to produce an environment that will be able to correct by itself the security defects that attacks would have revealed.

Status Quo:

- **Europe:** This is an understudied topic. Nevertheless, a French “grand défi” has recently been launched around the question “How to automate cybersecurity to make our systems resilient in the long run?”. An example of work comes from CTRL-A team at INRIA, which studies control techniques for the automated reaction to attacks. The group uses detection information to identify the appropriate defence and repair actions so that the system can remain operational, entirely or in a degraded mode.
- **International:** DARPA has recently launched a project (lead by BAE Systems) to model attacker behaviour in order to anticipate attacks, automate defence systems or even conduct correlation work relating to the attribution of attacks, but these issues remain unsolved today.

Estimated year of completion: 2030

Research aspect: Being able to automatically correct security defects that attacks would have revealed involves: (1) properly defining the system's security policy and how it is implemented, (2) detecting violations of this policy in real-time, (3) accurately diagnosing the causes and sources of these violations, (4) recovering the attacked system, and finally (5) automatically proposing changes to the policy and/or its implementation.

Industrial demand:

- Any business has to protect itself against potential attacks. This is a difficult and costly task. Automation would simplify this task and reduce its cost.
- Autonomous security is not currently operational.

Social aspect: Security and Privacy are two major concerns for the general public. The demand for secure computing environment is huge, both in the professional and in the personal sphere. Nevertheless, the mandatory skills are rare. Addressing this problem represents a long term effort in education and training. If bringing a better training to more people is crucial, automation may also be viewed as a way to tackle the problem.

Benefit for EU: The global geostrategic context is bad, and Europe is facing powerful countries (USA, China, Russia). In this context, the protection of European industrial assets is necessary.

The role of human operators remains essential for cyber Defence, but the automation of at least part of the response might be required in order to address large-scale, automated attacks.
SWOT Analysis: - **Strengths:** A strong European research community in formal methods, security policies, reasoning and logic, intrusion detection and alert correlation. - **Weaknesses:** This is a high-risk research topic. - **Opportunities:** Autonomous security is not currently operational. This is a subject on which Europe could take the research and then industrial lead. - **Threats:** The automation of the attack (e.g., offensive AI) could be operational before that of the Defence.
Domain (JRC Taxonomy): Operational Incident Handling and Digital Forensics
Sector (JRC Taxonomy): Potentially all, with special emphasis on Energy, Transportation, Digital Infrastructure, Finance, Supply Chain.
Relation to Emerging Technologies: Even if (for the time being) the feasibility remains an issue, AI-based systems could be able to autonomously handle advanced attack campaigns in the future. Faced with such automated attacks, a human response could be totally ineffective. Consequently, the automation of the response (at least defensively, as proposed here) will be a necessity.

Table 23: General information for Autonomous Security for Self-Protected Systems

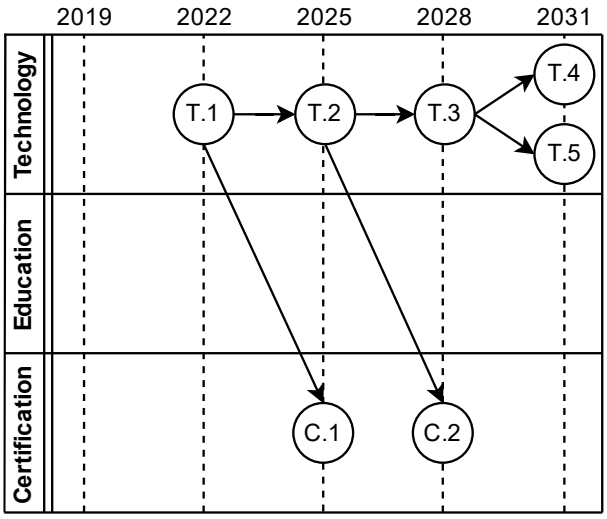


Figure 11: Timeline for expected completion of subgoals for Autonomous Security for Self-Protected Systems

Stage/Dimension *Tx for Technology* *Ex for Education* *Cx for certification*	**Sector (JRC)**	**Domain (JRC)**	**Regulation**
T1	Potentially all, with special importance in Energy, Transportation, Digital Infrastructure, Finance, Supply Chain	Operational Incident Handling and Digital Forensics	
	Description (incl. obstacles): Properly define the system's security policy and how it is implemented. Security policy refers to clear, comprehensive, and well-defined rules that regulate access to an organization's systems and the information included in them. A policy may be not that simple, and cases where two rules contradict each other are not rare. In this context, a proper definition of the policy would ask for a formal definition and verification of the set of rules. This formal specification of the policy could then be used to derive automatically the configuration of security tools able to enforce that policy.		
T2	Potentially all, with special importance in Energy, Transportation, Digital Infrastructure, Finance, Supply Chain	Operational Incident Handling and Digital Forensics	
	Description (incl. obstacles): Detect violations of security policies in real-time. Intrusion detection is essentially done at the network level. If, as expected in the near future, the traffic is more systematically encrypted, the analysis of the network packets would become de facto inoperative, apart from the header analysis. Therefore, it becomes important to study and design new mechanisms for monitoring information systems and producing alerts, at the application, middleware, operating system, and even firmware or hardware levels.		
T3	Potentially all, with special importance in Energy, Transportation, Digital Infrastructure,	Operational Incident Handling and Digital Forensics	

	Finance, Supply Chain		
	Description (incl. obstacles): Accurate diagnosis of the causes and sources of security policies violations. Current intrusion detection systems lead to a huge number of alerts, many of them being false positives. Thus, newly designed mechanisms should tackle this problem with the utmost attention. An additional step of alert correlation can improve detection. This step aims to improve the content of the alerts and thus to increase the “situation awareness” of the self-protected system.		
T4	Potentially all, with special importance in Energy, Transportation, Digital Infrastructure, Finance, Supply Chain	Operational Incident Handling and Digital Forensics	
	Description (incl. obstacles): Automatically propose changes to the policy and/or its implementation. When a security policy has been violated, two levels of reaction can be considered: (1) the attack may have succeeded because the policy was incorrect, in which case the policy must be amended, and new configurations of existing security mechanisms or even new security mechanisms must consequently be put in place; (2) the attack may also have succeeded because the enforcement of the policy was incorrect, in which case configuration errors of the security mechanism must be identified and corrected. As for the definition of the policy (see above), using formal methods can help in guaranteeing that the security properties requested by the policy are effectively insured at the policy level and at the enforcement level.		
T5	Potentially all, with special importance in Energy, Transportation, Digital Infrastructure, Finance, Supply Chain	Operational Incident Handling and Digital Forensics	
	Description (incl. obstacles): Recovering the attacked system In response to an attack and after updating the security policy, it is necessary to repair any damage that may have been caused in the system. The aim here is to identify the consequences of the attack		

	(diagnosis) and deploy the necessary corrective measures (patch management).		
C1	Potentially all, with special importance in Energy, Transportation, Digital Infrastructure, Finance, Supply Chain	Operational Incident Handling and Digital Forensics	
	Description (incl. obstacles): Detecting intrusions and anomalies: towards controlled false positive and false negatives rates. A critical point for anomaly or intrusion detection mechanisms is the final quantity of false alarms to be processed by security operators. As the large majority of the activities analysed are legal, even a low rate of false positives can lead to false alarms. Consequently, it would be useful to be able to control this rate of false positives, so that false alarms remain in reasonable numbers, so as not to drown out the true positives and to facilitate the work of analysts. This should be done without significantly penalizing the rate of false negatives. A balance must be found, which depends on the detection approach, the system under surveillance and the nature of the activities analysed.		
C2	Potentially all, with special importance in Energy, Transportation, Digital Infrastructure, Finance, Supply Chain	Operational Incident Handling and Digital Forensics	
	Description (incl. obstacles): Ensure that the defensive response to attacks is relevant. Responding to an attack includes adapting a given security policy. This adaptation must not introduce new vulnerabilities in the system, and must not lead to the restriction of legitimate rights. It is important to provide proof that these two constraints are fulfilled. Formal methods can help to this end.		

Table 24: Detailed description of Autonomous Security for Self-Protected Systems

8.3 Trustworthy Software

Title: Trustworthy Software

Problem description: Overall challenge: gain trust in the security of software, either by construction or by validation. In the context of Trustworthy Software, security is taken to mean that the software respects the confidentiality, integrity, and availability of data to be protected.

Final goal: A comprehensive collection of theories, techniques and tools that can enhance the trust in the security of our software.

Status Quo:

- **Europe:** Excellent status in academia in model-driven engineering, formal methods. High level of security certification in sub-domains (aeronautics, smart cards, etc.)
- **International:** Most major industrial stakeholders are based outside the EU (US, Israel, etc.). An important US and Canadian effort has been put into promoting formal methods in industrial projects.

Estimated year of completion: 2029

Research aspect: Trust in software can be obtained either by construction or by validation. The proposed approach is to explore both directions. This includes integrating security in a model-driven software engineering process, thereby giving substance to the security-by-design concept. In addition, the proposal is to develop formal methods with high guarantees of security properties. In terms of validation, this means developing analysis techniques for precise models of software behavior. This will enable the efficient detection of malware. In the long term, this could also provide new, more automated software security certification procedures.

Industrial demand: Strong in many sectors, including banking, finance, transportation, energy, health.

Social aspect: Increase the confidence that end users have in the digital economy. Guarantee the protection of privacy.

Benefit for EU: Win a competitive edge in other industrial sectors by an increase in software productivity, security and certification.

SWOT Analysis:

- **Strengths:** Strong academic level; successes in some industrial sectors
- **Weaknesses:** Some strong industrial EU stakeholders (Thales, SAP, Leonardo, Indra, etc.) but no global and worldwide undisputed leadership.
- **Opportunities:** In several other sectors (transportation in particular), major EU industrial leaders are ready to and interested in deploying formal methods.
- **Threats:** Other continents invest massively informal methods for cybersecurity. Risk of not being able to impose a European solution.

Domain (JRC Taxonomy): Assurance, audit and certification. Software and hardware Security Engineering. Theoretical foundations.
Sector (JRC Taxonomy): Defence, Energy, Financial, Health, Nuclear, Transportation, Space.
Relation to Emerging Technologies: The emergence of quantum computing will raise additional questions of how to construct and validate software systems. Techniques developed for classical Trustworthy Software will need to be reviewed in light of this emerging paradigm.

Table 25: General information for Trustworthy Software

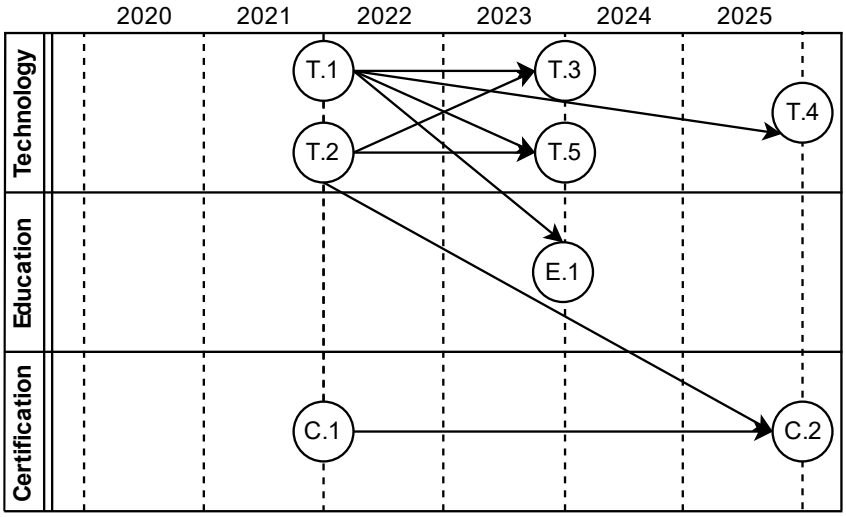


Figure 12: Timeline for expected completion of subgoals for Trustworthy Software

Stage/Dimension *Tx for Technology* *Ex for Education* *Cx for certification*	**Sector (JRC)**	**Domain (JRC)**	**Regulation**
T1	Equivalent to Table 25	Software and hardware security engineering. Theoretical foundations	
	Description (incl. obstacles): Model-driven engineering of secure software. Develop formal methods based software engineering techniques where security is integrated from the start. Use existing automation techniques (static analysis, model checking, SMT solvers,…) to scale the methods and increase their trustworthiness.		

T2	Equivalent to Table 25	Software and hardware security engineering. Theoretical foundations	
	Description (incl. obstacles): Binary analysis. Develop static and dynamic analysis techniques for analysing binary code. Analysis of unknown binaries is still a tedious task that is done in a mostly manual fashion. It should address the problem of binary function recognition, control flow graph recovery, and de-obfuscation by using approaches such as dynamic analysis, taint analysis and symbolic execution.		
T3	Equivalent to Table 25	Software and hardware security engineering. Theoretical foundations	
	Description (incl. obstacles): Evaluation and hardening of legacy code. This task is concerned with gaining trust in existing applications for which we might only assume to have the binary code. It will rely on the sub-goal on binary analysis to extract a precise model of binary code in order to enable its security evaluation. Going beyond mere evaluation we will also develop code transformation techniques for improving the security of a binary, in order to harden legacy code.		
T4	Equivalent to Table 25	Software and hardware security engineering. Theoretical foundations	
	Description (incl. obstacles): Explore the use of proof assistants and automatic software verification for validating security properties. The end result should be a concrete proposal for a framework giving substance to the term security-by-design.		
T5	Equivalent to Table 25	Software and hardware security engineering. Theoretical foundations	

	Description (incl. obstacles): Malware analysis. Develop static and dynamic analysis techniques for identifying malware based on its behavior, improving on today's signature-based techniques. These techniques must be able to locate and trigger the malicious part of the malware, even in the presence of anti-analysis and anti-detection techniques deployed in modern malware. Based on the behavioral analysis, extract models of the malware that can form the basis of a novel kind of malware detection tools.		
E1	Equivalent to Table 25	Software and hardware security engineering. Theoretical foundations	
	Description (incl. obstacles): Develop a secure software engineering course (both graduate and undergraduate level) that will use results from the challenge to teach secure-by-design software engineering and certification.		
C1	Defence, Energy, Financial, Health, Nuclear, Transportation, Space	Assurance, audit and certification, software and hardware security engineering	
	Description (incl. obstacles): Extend existing certification schemes to take into account recent advances in formal methods-based techniques. Take example from the aeronautics certification scheme where formal proofs can sometimes replace unit testing. This also includes identifying processes where formal methods and automatization can aid in the security certification.		
C2	Defence, Energy, Financial, Health, Nuclear, Transportation, Space	Assurance, audit and certification, software and hardware security engineering	
	Description (incl. obstacles): Imagine, develop and describe new certification schemes based on formal methods for security that exploit the novel software engineering techniques developed in this challenge to complement or perhaps even replace existing process-oriented certification schemes.		

Table 26: Detailed description of Trustworthy Software

8.4 Quantum Information Technology

Title: Quantum Information Technology

Problem description: Quantum theory is entering the area of information technology. Quantum communication is emerging as a technology and it is likely that building a universal quantum computer will become feasible in the next decades. This raises several questions in terms of cybersecurity: how can quantum communication help to improve cybersecurity and, conversely what are the security threats brought by this new way of computing? Similarly, how much does it cost to migrate to quantum resistant technologies?

Final goal: The final goal is to create a theoretical basis and a set of practical solutions for secure incorporation of quantum technologies as well as ensuring that existing systems are secure enough to withstand quantum adversaries.

Status Quo:

- **Europe:** The importance of quantum information technology is well acknowledged by European countries, which do invest in it separately and through global European funds. Europe has strong knowledge in the area and centres doing quantum computing research.
- **International:** Internationally countries across the world are concerned with emergence of quantum technologies and invest a lot (USA, China, Canada, as well as Japan, South Korea, Saudi Arabia, Russia etc.). But it is more important to underline that the top tech companies (Google, IBM, Intel, Microsoft, etc.) also invest in this technologies and these investments often are higher than the ones made by countries. Most of these companies are not European.

Estimated year of completion: 2030

Research aspect: Quantum information technology brings several aspects to be dealt with. We outline the following three which could be seen as the most pressing today: 1) Quantum communication and secure key distribution; 2) Post-quantum cryptography; 3) Security of computing platforms mixing classical and quantum computation.

We must underline that integration of quantum technology to existing information systems could be seen as quite a novel approach, and thus, may result in a number of new research aspects once the integration will become stronger.

Industrial demand:

- Industry needs a secure way for communication and protection of its sensitive data
- Quantum computers once implemented will threaten the existing cryptographic schemas. The industry needs new cryptographic schemas strong enough to withstands quantum adversary. In addition, those technologies need to be embedded in legacy systems.
- Quantum technology is appealing for implementation, but must be carefully incorporated in the existing classical networks, to ensure that all risks are well understood and properly treated.

Social aspect: Quantum information technology is both opportunity for stronger security and dangerous threat for it. It especially targets the existing cryptographic systems which ensure confidentiality of private data, as well as integrity of most transactions. Access of the society to the digital services will be severely impacted, significantly reducing the public trust in digital economy.
Benefit for EU: It is difficult to overestimate possible benefits for EU from possessing quantum information technologies. Industry and society will be severely impacted if this technology is not timely and correctly implemented. Loosing quantum race may put a country in a weak position with respect to the winner, threatening the work of security and intelligence agencies, ability to protect basic human rights, correctness of operation of governmental institutes, etc.
SWOT Analysis: - **Strengths:** Strong knowledge of European research community in quantum information technologies and quantum cryptography. Acknowledgement of its importance by the high governmental agencies - **Weaknesses:** Many international (mostly US) corporates invest much higher amount of money into the development of quantum information technologies than Member States and EU, in general. Some of these companies demonstrate better progress with respect to the EU. - **Opportunities:** It is of paramount importance to possess the knowledge of quantum information technologies, as it may impact all spheres of life. This also means huge market demand (in the nearest future) for the quantum information solutions. - **Threats:** Loosing the quantum race. Underinvestment. Brain drain and technology leakage (e.g., by corporates who buy technology and people).
Domain (JRC Taxonomy): Cryptology; Security Management and Governance; Network and Distributed Systems
Sector (JRC Taxonomy): All
Relation to Emerging Technologies: Quantum computing is by itself an emerging technology, which is only recently proved to be soon implemented in practices. Some cutting edge cryptographic techniques could be outlined here, like lattice-based, code-based, and multivariate-based primitives.

Table 27: General information for Quantum Information Technology

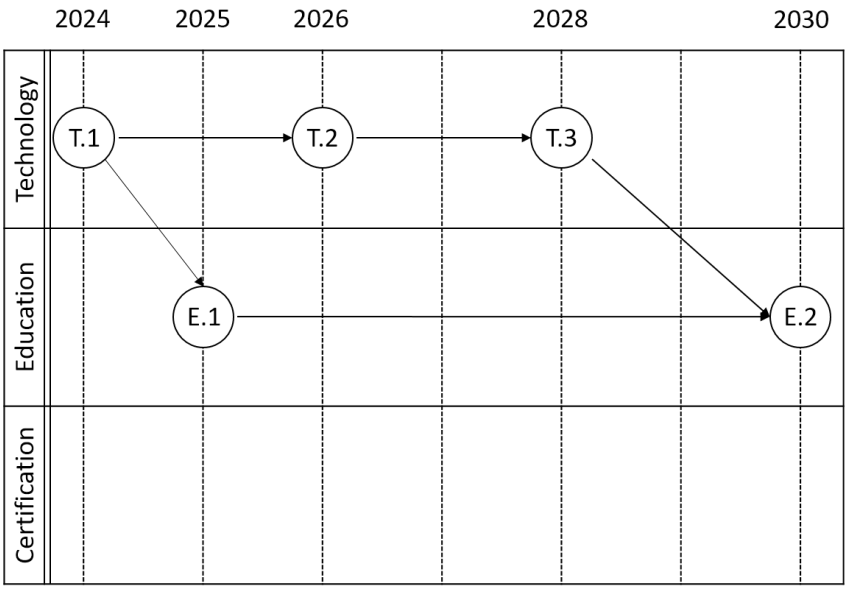


Figure 13: Timeline for expected completion of subgoals for Quantum Information Technology

Stage/Dimension *Tx for Technology* *Ex for Education* *Cx for certification*	**Sector (JRC)**	**Domain (JRC)**	**Regulation**
T1	Digital Infrastructure	Cryptography; Security Management and Governance; Network and Distributed Systems	
	Description (incl. obstacles): Quantum communication and secure key distribution. With quantum communication, it is possible to construct an unconditionally secure key distribution protocol (known as the BB84 protocol). This means that even an all-powerful (potentially quantum) adversary cannot break the scheme. More precisely, any attempt to access a (symmetric) cryptographic key when it is exchanged tanks to quantum communication, would be detected. This offers long-term security, but can only be used for a limited number of applications, such as key distribution described above, because of deployment constraints and is thus usually combined with standard or quantum-safe cryptography. In Europe and in Asia, quantum networks are being developed in order to be able to perform unconditional quantum key distribution protocols. Currently, these protocols only work on a limited distance of about 50-150 km, even if some experiments now reach a distance of about 1000km. Creating large-scale networks requires trusted nodes (which can be dangerous from a cryptographic point of view) or quantum repeaters. Quantum repeaters are technologically out of reach today, but seem easier to build than a full quantum computer		

	and could arrive in a near future.		
T2	All	Cryptography	
	Description (incl. obstacles): Post-quantum cryptography. Most asymmetric cryptography used today is based either on the hardness of factoring or computing discrete logarithms. Unfortunately, these problems are both known to be efficiently solvable by a quantum computer. It is important to investigate from now quantum-resistant cryptography, as some information that is encrypted today may still be sensitive in, say, 50 years. New mathematical problems, that cannot be solved using a quantum computer, must thus be found and studied. Several good candidates have already been proposed, such as lattice-based, code-based, and multivariate-based primitives. It is urgent to perform an in-depth security analysis of these new schemes.		
T3	All	Cryptography; Security Management and Governance; Network and Distributed Systems	
	Description (incl. obstacles): Security of computing platforms mixing classical and quantum computation. Given that a full quantum computer is still some years or decades away, it seems more likely that the first quantum computing platform will be a classical architecture integrating some quantum elements. This then calls for a general assessment of the security properties of such an architecture, and of techniques for exploiting this new architecture to develop secure quantum software.		
E1	All	Cryptography	
	Description (incl. obstacles): Quantum and post quantum cryptography professionals. Increased quantity of skilful professionals should be raised with knowledge of quantum computing and quantum cryptography. These professionals will have to advance the technology as well as serve the corresponding operating quantum mechanisms and systems.		

E2	All	Security Management and Governance; Network and Distributed Systems	
	A new generation of (cyber) security professionals should be raised with the knowledge of both quantum theory and information technology. These professionals will ensure that the integrated quantum-classical IT systems are well protected as from classical, as well as from quantum-related threats, and the hybrid ones.		

Table 28: Detailed description for Quantum Information Technology

8.5 5G Security

Title: 5G Security
Problem description: 5G technology does not only provide a new, faster and more reliable communication facilities, it also opens the possibility for much higher amount of (sensitive) data to be transferred, connecting different types of infrastructure and applying novel technologies. This data should be protected from the possible abuse by malicious technology and software providers or dishonest network facility providers.
Final goal: Although a number of issues should be solved, in order to ensure adequate protection for the new communication technology, the overall goal could be stated as to protect the data during its transmission via 5G networks.
Status Quo: - **Europe:** European companies lag behind their non-European competitors in the development of solutions for 5G technologies. This leads to heavy reliance of Europe on non-European technology providers, who in turn will get access to vast amount of data belonging to European citizens, industries and governments. - **International:** US and Chinese companies possess 5G technological solutions that are ready for or being deployed.
Estimated year of completion: 2030
Research aspect: 5G security includes a number of aspects which require specific attention: 1) security orchestration and management (dealing with different security requirements, different operators, different technologies); 2) resilience against flash of network traffic (with potential abuse as DDoS); 3) end-to-end security (network and application level); 4) consistency of subscriber level of protection; 5) adaptive security (new technologies, new threats); 6) certification of 5G hardware and software.
Industrial demand: • Industry will rely on 5G networks to share its sensitive data • 5G providers will have to ensure a high level of protection for their customers and cooperate with other similar providers with different level of security. • 5G providers will rely on (untrusted) 5G technology providers and would like to be assured that proper quality of protection is provided and the applied solution do not violate security requirements.
Social aspect: 5G will have huge impact on the life of the generic public. Clearly, personal data will be exchanged between users and industry and processed further. As with growing reliance of the public on IT services the demand for privacy raises, the pressure on communication providers to protect the data in transfer is increasing as well. Thus, security of the 5G technologies will have immense impact on the trust in IT technology in general.
Benefit for EU: Apart of direct benefit for the European industry in increasing the

competitiveness of their 5G technological solutions, the following benefits should be also outlined. First of all, this will let the EU to be able to protect and control its data, ensuring that the basic rights of its citizens are guaranteed and the EU laws are enforced. Good knowledge of 5G security will also ensure that the technologies adapted by EU industry from external technology providers is genuine, free from possible backdoors and complies with EU standards and regulations. High level of security of 5G communication networks will also increase the trust of citizens and business in the IT technologies, as well as in the EU's capability to protect its values.
SWOT Analysis: - **Strengths:** Strong knowledge of the European (academic and industrial) community in security policies, security management, communication security, intrusion detection and malware analysis, security engineering, etc. Some EU companies are developing their own 5G network technologies. - A strong European research community informal methods, security policies, reasoning and logic, intrusion detection and alert correlation. Some industrial key actors in the security business. - **Weaknesses:** European technologies for 5G is lagging behind the most advanced companies from US and China. - **Opportunities:** The 5G technology market is promised to be huge and will be operational only in the nearest future. - **Threats:** Superiority of the current 5G leaders could be very hard to catch up with. Moreover, the major investments and human resources could be attracted by the leading (non-EU) companies.
Domain (JRC Taxonomy): Assurance, Audit, and Certification; Security Management and Governance; Network and Distributed Systems; Software and Hardware Security Engineering; Cryptology
Sector (JRC Taxonomy): Digital Infrastructure, Supply Chain.
Relation to Emerging Technologies: 5G network uses various cutting edge technologies for providing the most up-to-date and long lasting communication service. Thus, it employs Cloud Computing, Artificial Intelligence, IoT technologies, as well as Software Defined Networks, Network Function Virtualization, Multiple-Input and Multiple-Output, etc. The usage of these cutting edge technologies results in a number of benefits for the new generation network, but also causes a number of problems for security because of increased attack surface, which may (and, most probably, will) expand in the future.

Table 29: General information for 5G Security

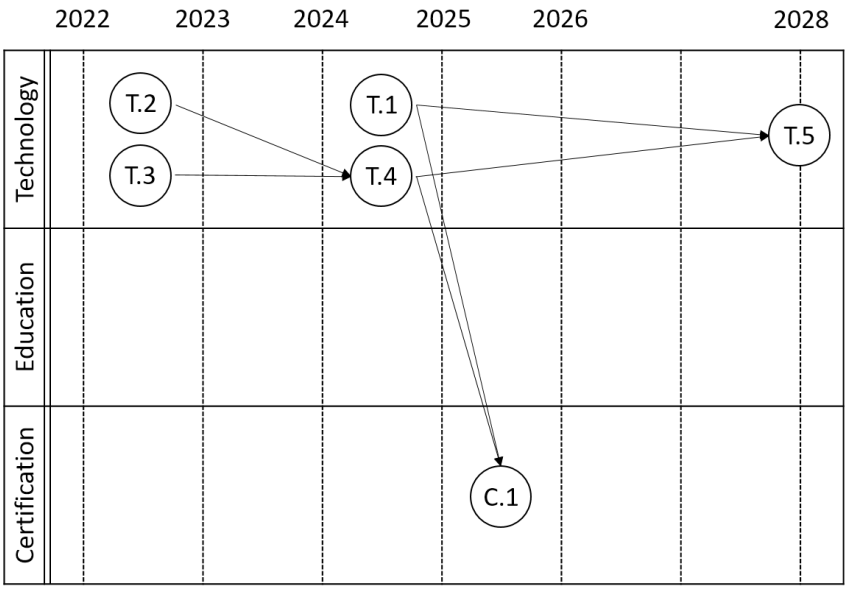


Figure 14: Timeline for expected completion of subgoals of 5G Security

Stage/Dimension *Tx for Technology* *Ex for Education* *Cx for certification*	**Sector (JRC)**	**Domain (JRC)**	**Regulation**
T1	Digital Infrastructure, Supply Chain	Security Management and Governance; Network and Distributed Systems	
	Description (incl. obstacles): Security orchestration and management. 5G network will connect various infrastructures (such as IoT, Cloud, smart grids, etc.) and rely on various technologies (e.g., SDN, NFV, AI, MIMO, etc.). Moreover, various parts of the network may belong to different stakeholders and, thus, have different security measures installed and ensure different quality of protection. The network must be well orchestrated in order to ensure good security of communication (according to the system security requirements).		
T2	Digital Infrastructure	Network and Distributed Systems	
	Description (incl. obstacles): Resilience against flash of network traffic. 5G networks are aimed to connect huge amount of devices (including IoT). Large swings of traffic (either unintentional or intentional) are		

	foreseeable. The network must be reliable enough to deal with such flash of network traffic and be prepared that malicious actors will try to abuse high connectivity of devices to cause latencies and drop downs of the network.		
T3	Digital Infrastructure	Cryptology (Cryptography and Cryptanalysis)	
	Description (incl. obstacles): End-to-end security (network and application level). Previous generations of the cell communication networks do not provide cryptographic integrity protection for the user data. Therefore, there is the need to provide protection at transport and application levels. For some applications (e.g., for IoT) cryptography at application layer could cause too much overhead in data transmission (and processing) and delays. Therefore, network level security could be applied for such networks.		
T4	Digital Infrastructure, Supply Chain	Security Management and Governance; Network and Distributed Systems	
	Description (incl. obstacles): Consistency of subscriber level of protection. Network subscriber will have different security requirements which have to be ensured even if the subscriber is moved to another network or to another operator (e.g., roaming). Since the networks may provide different levels of protection, the security policies must be shared between network operators and the consistency of subscriber level of protection must be ensured. The methods and tools ensuring secure transfer of a subscriber should be developed.		
T5	Digital Infrastructure,	Security Management and Governance; Network and Distributed Systems	
	Description (incl. obstacles): Adaptive security (new technologies, new threats). 5G network technologies are only to be implemented in the nearest future, so they are to be the dominant means of mobile communication for years. With the rapid development of IT technologies and even more rapid adaptation of attackers, 5G networks technologies must be developed agile enough to ensure security even if new IT technologies		

<table>
<tr><td></td><td colspan="3">are to be applied. In addition, research is required to ensure that these networks will be ready to withstand novel, probably, not yet existing security threats.</td></tr>
<tr><td rowspan="2">C1</td><td>Digital Infrastructure, Supply Chain</td><td>Assurance, Audit, and Certification;</td><td></td></tr>
<tr><td colspan="3">Description (incl. obstacles):
Certification of 5G hardware and software.
Since huge amount of sensitive data are to be passing through 5G networks, there is a need to ensure that the technologies it uses (both software and hardware) are reliable, do not have backdoors, and satisfy European requirements. Thus, certain assurance procedures must be established. Moreover, since 5G networks are critical for the well-being of European citizens and business, a mandatory certification could be applied to enforce usage of secure products only.</td></tr>
</table>

Table 30: Detailed description for 5G Security

8.6 Trusted Hardware/Software Co-Design

Title: Trusted Hardware/Software Co-Design

Problem description: Computing platforms, i.e., hardware and low-level software components such as operating system, hypervisor, or firmware, play a fundamental role in securing applications and data hosted on computers. However, such platforms are more and more complex and not exempt from vulnerabilities. The challenge is to enhance the security of computing platforms, which requires paying attention to the interactions between hardware and software. We must consider both hardware and software attacks. Notice that software attacks can also exploit hardware vulnerabilities, e.g., vulnerabilities affecting the microarchitecture.

Final goal: The final objective is to provide a security-enhanced trusted computing platform that can resist intrusions targeting the platform itself or the hosted applications and data by co-designing hardware/software security mechanisms. However, adding additional security mechanisms will increase the complexity of the computing platform, possibly leading to vulnerabilities. Thus, we should also develop attack methodologies for systematic security testing of computing platforms. A long-term objective to increase the trust in the computing platform is to use formal methods to specify and verify the security mechanisms of the platform, especially those involving hardware and software interactions.

Status Quo:

- **Europe:** Multiple research groups in Europe (e.g., Secure Systems Group at Graz University of Technology, Imec-DistriNet at KU Leuven, SAFARI at ETH Zürich, or VUSec at Vrije Universiteit Amsterdam) have been highly active in identifying vulnerabilities affecting the microarchitecture of processors and developing software attacks that exploit these hardware vulnerabilities. However, less attention has been paid to the design of defensive approaches.
- **International:** Many research groups in the USA are working actively on attacks (e.g., the University of Michigan, College of William and Mary, Columbia University, or the Vernam Lab at Worcester Polytechnic Institute) or in developing hardware/software security mechanisms (e.g., CSAIL at MIT, the Department of Computer Science and Engineering at the Pennsylvania State University, the EECS Department at UC Berkeley, the University of Illinois–Urbana Champaign or the Sun Security Laboratory at George Mason University). Security groups in Asia (e.g., the University of Adelaide in Australia, CySecLab at KAIST in Korea, or the COMPAS Security Lab at Southern University of Science and Technology in China) are also highly active in that domain. However, these groups do not cover the whole hardware/software stack systematically. CHERI (Capability Hardware Enhanced RISC Instructions) is one of the few research projects covering both software and hardware aspects, from hardware design to the use of formal methods for validation, through the development of a software stack taking advantage of hardware extensions. CHERI is a joint research project of SRI International and the University of Cambridge to revisit fundamental design choices in hardware and software to improve system security using capability-based processor architectures. Arm has just shipped its CHERI-enabled Morello prototype processor in January 2022. However, capabilities cannot protect the system against all types of attacks (e.g., side-channel attacks).

Estimated year of completion: 2030

Research aspect: Enhancing the security of computing platforms first implies identifying the vulnerabilities affecting them and evaluating the feasibility of hardware and software attacks exploiting such vulnerabilities. Automating this complex and tedious task is crucial, especially for identifying microarchitectural vulnerabilities and resulting side-channel attacks. It is necessary to propose new software/hardware co-designed security mechanisms to prevent the exploitation of vulnerabilities. Finally, it is important to develop hardware support for host-based intrusion detection and reaction. The main challenges are to isolate the detection and reaction mechanisms while bridging the semantic gap resulting from this isolation.
Industrial demand: There is a strong demand in many sectors, including Defence, safety-critical applications, and governmental. Hardware manufacturers are also more and more inclined to embed security mechanisms into their processors (e.g., Arm TrustZone, AMD PSP, Intel SGX, or CET). However, these solutions offer limited isolation (e.g., against side-channel attacks) and lack of formal validation.
Social aspect: Enhancing the security of computing platforms will significantly improve the security of user applications and data. Thus, it increases the confidence that end users have in the digital economy and contributes to privacy protection.
Benefit for EU: Designing highly trusted computing platforms will contribute to developing sovereign solutions, which is critical in the Defence sector.
SWOT Analysis: - **Strengths:** A strong European research community in formal methods and hardware security. Some industrial leaders in defence sector that could collaborate on the research effort and industrialize the proposed solution. - **Weaknesses:** Hardware and software security are still often considered as separate issues, addressed by distinct communities - **Opportunities:** Hardware vendors are more inclined to embed new security features to face the increasing user demand for security. - **Threats:** Most of the hardware and software components of computing platforms commonly used in all the sectors of the EU economy are developed and industrialized by non-EU companies, which are also developing similar approaches.
Domain (JRC Taxonomy): Software and Hardware Security Engineering
Sector (JRC Taxonomy): Potentially all, with special importance in Defence, Government, Nuclear, Safety and Security
Relation to Emerging Technologies: AI support for the automatic identification of vulnerabilities and attacks affecting computing platforms. Security of computing platforms mixing classical and quantum computations.

Table 31: General information for Hardware/Software Co-Design for Computing Platforms

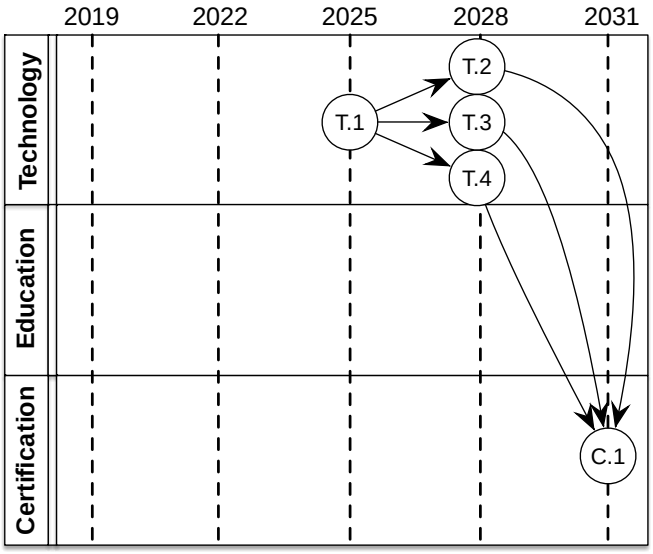


Figure 15: Timeline for expected completion of subgoals for Hardware/Software Co-Design of a Trusted Computing Platform

Stage/Dimension *Tx for Technology* *Ex for Education* *Cx for certification*	**Sector (JRC)**	**Domain (JRC)**	**Regulation**
T1	Potentially all, with special importance in Defence, Government, Nuclear, Safety and Security	Software and hardware security engineering.	
	Description (incl. obstacles): Automating the analysis of attacks against computer platforms. Automating the analysis of software attacks (e.g., side-channel attacks) is still an open problem today. It is necessary to assess whether hardware and software vulnerabilities are exploitable, given the code of an application. A black-box approach, which does not rely on an explicit model of the microarchitecture but relies on techniques derived from artificial intelligence, seems to be promising. This automation offers interesting scientific perspectives and corresponds to an industrial need in the certification process. Indeed, in the context of security evaluations carried out under constraints of time (e.g., evaluations following the French CSPN schema), the expert does not have the necessary resources to carry out an in-depth analysis of the microarchitecture.		
T2	Potentially all, with special importance in	Software and hardware security	

	Defence, Government, Nuclear, Safety and Security	engineering.	
	Description (incl. obstacles): Hardware/software co-design of preventive security mechanisms. Designing new security mechanisms relying on hardware features is appealing since attackers cannot modify hardware components, making them more robust against software attacks. However, the processor must adopt a conservative behavior only when it handles confidential data to preserve performance. To do this, it must rely on the software (e.g., compiler, OS, or hypervisors), which must tell it which data to protect. In general, it will be necessary to revise the traditional contract between the hardware and the software to guarantee strong isolation while minimizing the overhead of the protections. A long-term objective is to rely on formal methods approaches from the design and development phase of hardware and software, which would help the certification phase described in C1.		
T3	Potentially all, with special importance in Defence, Government, Nuclear, Safety and Security	Software and hardware security engineering.	
	Description (incl. obstacles): Hardware support for Host-based Intrusion Detection and Reaction. Trusted computing platforms should not only prevent existing intrusions but should also be able to detect and react to any security threat. We should provide such platforms with detection and reaction capabilities implemented at the host level. We must also protect such mechanisms from attacks targeting the platform by isolating them from other components, using new or existing hardware features. However, isolation creates a semantic gap between the monitored host and the monitor that, to date, remains a significant challenge for this type of approach. Using hardware support to implement fine-grained countermeasures (e.g., changing the state of an application) and isolating the reaction mechanism is also appealing, both from a scientific and an industrial application perspective.		
T4	Potentially all, with special importance in Defence, Government, Nuclear, Safety and Security	Software and hardware security engineering.	
	Description (incl. obstacles): Trusted Isolation Mechanisms.		

	Modern processors increasingly embed TEEs or enclaves, which are execution environments isolated within the processor. Such TEEs theoretically guarantee the confidentiality and integrity of data hosted and manipulated in these environments. However, unlike approaches that use external components, TEEs share resources (CPU, cache, memory, peripherals) with the classic execution environment. Evaluating the security guarantees these environments provide remains an open problem. Recent work has confirmed that most hardware implementations are not resistant to auxiliary channel attacks. There is a need to develop more robust isolation mechanisms for TEEs.		
C1	Potentially all, with special importance in Defence, Government, Nuclear, Safety and Security	Software and hardware security engineering, Assurance, Audit, and Certification	
	Description (incl. obstacles): Formal Specification and Verification of Hardware/Software Security Mechanisms To increase confidence in computing platforms, we must propose approaches for developing hardware components ensuring that: 1. these components behave according to a formal specification. 2. these components can guarantee some security properties. This last point requires the implementation of security mechanisms within these components and verifying that this implementation enforces the expected security properties. This task is more complex when some security mechanisms need cooperation between the hardware, which provides security primitives, and the software, which must use them correctly to ensure the security property. One of the challenges is verifying that the hardware implementation, whether an ASIC or a soft-core implemented on FPGA, respects this specification and the security properties.		

Table 32: Detailed description of Hardware/Software Co-Design of a Trusted Computing Platform

8.7 Towards Secure Next-Generation Computing Architectures

Global technical advances in computing push into the application domains with high speed and cybersecurity has to be supported to keep pace and recover Europe's technical sovereignty in tomorrow's driving technologies. IoT devices, processors and system-on-chips are sourced in global supply chains and it is currently not possible to ensure that only trustworthy components are integrated in neuralgic points of the systems. AI enhances more and more embedded devices, supported by neuromorphic computing. The corresponding security technologies are currently lacking to protect the computation and the data. High-performance computing is moving from closed environments to open architectures and even the edge without taking security into account to the necessary extent.

It becomes important to research new security technologies and integrate them into NGC components and systems to ensure European technical sovereignty while leveraging global trends. Europe has globally leading players in cybersecurity research and the smartcard industry meaning that substantial security know-how is available but it is difficult for non-security industry to integrate next-generation security technologies into their core components. The open-source community is developing more and more hardware, but it is not ready for commercial use and transfer into the applications in society.

The processes and environments for open-source software, like Linux, matured over the last two decades such that they are in widespread productive use, while open hardware recently started moving out of the research community towards a widespread industrialisation. This process requires material for manufacturing and has higher turnaround times such that a collective effort and also funding support is necessary to go this step and reach a similar maturity to enable European Technological Sovereignty. This, in turn, requires research into how to design next-generation open architectures and, beyond that, novel computing platforms based on eg. biology or quantum physics.

Chapter 9 Open-Source Hardware and Software

In line with the ambitious mission of strengthening EU's digital sovereignty, SPARTA embraces the innovative philosophy empowered by open-source hardware and software.

What is open-source?

Open-source strategies generally benefit citizens, industries, and governments in various ways. First of all, publicly disclosed implementations enable sharing of knowledge and skills from communities at large which exceed the boundaries caused by the limited number of developers working on a closed-source product. Anyone is eligible to analyse, review, and contribute to public software and hardware under open-source licenses. Moreover, free software and hardware can be accessed, reused, and modified mostly without financial costs by any interested stakeholder to match their use-case. This accelerates innovation and allows citizens and SMEs to benefit from the advantages of automation that would otherwise be unaffordable. Furthermore, open-source products remove the danger of vendor lock-in and enable fair competition between available implementations.

What is the relationship with cybersecurity?

Lastly, open-source empowers transparency and strengthens the security of publicly disclosed technologies. The transparency of software and hardware that is open-sourced increases the population's trust in digital services, which is key to prosperous innovation. Due to their public availability, independent audits may be conducted at any time for certifying that open-source products comply to their specification, and, additionally, for detecting further flaws. This is an unmeasurable benefit for hardening digital systems since potentially critical flaws are discovered, and, therefore, addressed faster. Moreover, open-source repositories may be freely analysed by independent advocates for secure and privacy-preserving technologies. This represents an advantage compared to closed-source products whose security is evaluated only on demand and at the cost of potentially considerable financial and human resources. Furthermore, when linked with bug-bounty programs, open-source products benefit from an even richer security evaluation, as now security bounty hunters have an added incentive to get involved and contribute.

Surprisingly, communities may not be aware of the added security benefits of open-source hardware and software. Based on an ongoing survey campaign on open-source software and hardware conducted by Fraunhofer ISI in collaboration with the Commission, preliminary results show that security or transparency are not among the reasons EU stakeholders would invest and contribute to public technologies. This is worrying and signals the urge to spread awareness on the security benefits of the open-source philosophy across the EU industries.

Why is it relevant for EU's digital sovereignty?

SPARTA proposes and prototypes key cybersecurity technologies that empower EU's digital sovereignty towards a digital single market. Open-source plays a key role in achieving this ambitious goal. Benefitting from open-source technologies encourages the coexistence of multiple implementations which enables one's freedom to choose the optimal solution. Moreover, user-centric data policies lie at the foundation of the EU whose one of the most prominent values is user privacy. Open-source strategies enforce this value, as citizens may inspect specific implementations of interest and learn in what way these process their data. Furthermore, open-source empowers inter-operability, which is one of the most important challenges in a society as diverse as the EU to function sustainably

Chapter 10 SPARTA Roadmap Challenge Priorities

This chapter proposes an ordering of the aforementioned SPARTA challenges with respect to their priority towards the SPARTA mission of strengthening EU's digital autonomy. The prioritization was produced based on input collected from the pilot, its network of partners, associates & friends. Under normal circumstances, we would have relied on in-person SPARTA workshops and events to stimulate the audience and gather feedback on the roadmap. However, since the past year has hindered such events, we performed the survey using an online questionnaire that we published in the SPARTA network.

The questionnaire contains an entry for each roadmap challenge separated in three categories: Emerging Challenges, Transversal Challenges, and Program Challenges which reflect the three types of challenges addressed by the SPARTA roadmap. Each entry encloses a rating scale ranging from 1 to 5, 1 representing a low priority, 5 representing a high priority, with the value 3 (neutral) as default. Moreover, each questionnaire item offers a text box meant to collect textual justification for one's corresponding rating. The present roadmap document was available to participants for further assistance at all stages of the questionnaire.

We organized the surveying campaign over the course of two months during which we received a total of 19 submissions: 15 from SPARTA partners and 4 from SPARTA associates & friends. However, this is merely a first step towards prioritization. We are aware, that the result might be biased because in this very first step mostly SPARTA members were asked to prioritize. Nevertheless, the result shows an initial tendency for ranking. We will gradually expand the circle in the next steps as we intend to collect feedback on setting priorities from other SPARTA network partners as well as from the cybersecurity community. Results from the updates of national research agendas on cybersecurity, among others in Germany, to be expected this year, will be taken in consideration as well. Moreover, findings from the action requirements due to the COVID-19 pandemic will have an impact on prioritization as well.

For our first surveying campaign we set up an input gathering window of two months during which we encouraged the SPARTA partners to fill out the questionnaire. We collected the feedback and computed the average rating for each challenge by summing up all individual ratings per challenge and dividing the sum by the total number of submissions. The resulting order sorted descending from the highest rating to the lowest is the following:

Rank	Roadmap Challenge	Average Rating
1	Secure and Fair AI Systems for the Citizen	4.2
2	Trustworthy Software	4.1
3	User-Centric Data Governance	4.1
4	Full-Spectrum Situational Awareness	4.1
5	Education and Training	4.05
6	5G Security	4.05
7	Security and Safety Co-Assessment	3.9
8	Next-generation computing architectures	3.85

Rank	Roadmap Challenge	Average Rating
9	High-Assurance Intelligent Infrastructure Toolkit	3.8
10	Certification Organization and Support	3.75
11	Complex Dynamic Systems of Systems	3.6
12	Autonomous Security for Self-Protected Systems	3.4
13	Quantum Information Technology	3.4

The challenge of Secure and Fair AI Systems for the Citizen was ranked with the highest priority for strengthening digital sovereignty in the EU. The participants of the survey stated that AI and ML technologies are envisioned to have a great impact within the EU in the following years. With recently large investments made in AI, the technology will become ubiquitous across industries in the next decade. For that reason, the participants of the survey argued, that cybersecurity is key to guarantee the fairness and security of AI algorithms and systems. They further argue that in order to create and maintain trust in AI systems we need to be careful in the way they are designed, implemented and taking special care of the quality and fairness of the data used to make the inferences. Furthermore, to move forward towards digital sovereignty, the participants argued, it is of high importance the EU relies on secure and certified AI systems that comply to European values such as privacy and transparency. This will increase trust and, therefore, accelerate adoption of AI in the EU.

Trustworthy Software comes as SPARTA's roadmap challenge with the second highest priority towards digital sovereignty. The participants in the survey justify their assessment with the observation that software is running on devices and platforms that are used in almost every aspect of life. They argued that software is not yet fully understood by non-specialized communities, which makes digital products and services less trusted. Therefore, it is of outmost importance to guarantee that software running within the EU is free of backdoors and flaws to ensure their secure, safe, and reliable execution, which is key in order to be sovereign. In addition, the participants argued, as it is unrealistic that EU or any member state be autonomous in software production, it is especially relevant for digital autonomy to have strict assessment and certification processes and being able to identify trustworthy software. One participant stated, that without trustworthy tools and software that allows you to execute your autonomy, you are not really autonomous.

Both the previous challenges have high implications on user's control over their personal data and their interaction with the respective technology. As these values lie at the foundation of the EU, User-Centric Data Governance represents a high SPARTA priority for digital sovereignty, occupying the third place in the ranking. The participants argued, that autonomy should put the user in the centre. Although the EU is generally perceived as a role model regarding policies that protect citizens in digital environments, building more user-centric technologies should increase on-line privacy, essentially by saving citizens from having to make difficult privacy decisions, the ramifications of which they cannot understand. Moreover, user-centric technologies might represent competitive advantage among service providers in the near future as regulations push data control to the user and trends such as self-sovereign identity enable user-centric models for data governance.

Another highly ranked cybersecurity challenge addresses the problem of Full Spectrum Situational Awareness. The participants of the survey argued that such technologies would empower EU cybersecurity institutions to address complex, advanced cyber threats via wide data/information sharing which is a general need for digital autonomy. In addition, they argued that predicting full-spectrum designed cyberattacks requires higher cross-sector and cross-border knowledge contribution that lift defences from national to EU level. Therefore, they stated, that we need technologies that facilitate these aspects. There is a long-term need for improving situational

awareness of the environment and of critical infrastructure in particular. Current, now outdated, methodology has only a limited vision of the environment and can't provide adequate security services.

We have here commented on the four challenges that ranked highest in our internal SPARTA survey. However, the SPARTA roadmap committee would like to stress that the remaining challenges are considered important for strengthening digital sovereignty as well.

Chapter 11 SPARTA Roadmap and the JRC Taxonomy

This chapter contains the projection of the Roadmap Challenges (except the emerging challenges Towards Secure Next-Generation Computing Architectures, 5G Security, Trusted Hardware/Software Co-Design, and Quantum IT) over each dimension of the JRC taxonomy, showing the coverage of our roadmap over cybersecurity domains, technologies, as well as sectors where these can be applied.

Domains/Challenges	T-SHARK	CAPE	HAII-T	SAFAIR	Education and Training	Certification Org. and Support	User-Centric Data Governance	Autonomous Security	Trustworthy Software
Assurance, Audit and Certification		■	■			■			■
Cryptology			■						
Data Security and Privacy	■	■	■	■	■		■		
Education and Training		■							
Operational Incident Handling and Data Forensics								■	
Human Aspects		■		■					
Identity and Access Management			■						
Security Mgmt. and Governance									
Network and Distributed Systems			■						
Software and Hardware Security Engineering			■						■
Security Measurements	■								
Legal Aspects		■		■					
Theoretical Foundations		■	■	■					■
Trust Management, Assurance and Accountability			■						

Table 33: JRC Research Domains covered by SPARTA roadmap challenges

Applications and Technologies /Challenges	T-SHARK	CAPE	HAII-T	SAFAIR	Education and Training	Certification Org. and Support	User-Centric Data Governance	Autonomous Security	Trustworthy Software
Artificial Intelligence	■			■				■	
Big Data	■			■			■		
Blockchain and Distributed Ledger Technology									■
Cloud and Virtualization			■				■		■
Embedded Systems			■						■
Hardware Technology (RFID, chips, sensors, routers…)		■							
Industrial Control Systems (SCADA)						■			
Information Systems	■			■	■	■		■	■
Internet of Things		■	■			■			■
Mobile Devices			■						
Operating Systems			■					■	■
Pervasive Systems									
Quantum Technologies									
Robotics		■							
Satellite Systems and Applications									
Supply Chain						■			
Vehicular Systems		■				■			■

Table 34: JRC Applications and Technologies covered by SPARTA roadmap challenges

Sectors/Challenges	T-SHARK	CAPE	HAII-T	SAFAIR	Education and Training	Certification Org. and Support	User-Centric Data Governance	Autonomous Security	Trustworthy Security
Audiovisual and Media					■	■	■		
Defence	■					■	■		■
Digital Infrastructure	■				■	■	■	■	
Energy		■	■	■		■	■	■	■
Financial		■		■		■	■	■	■
Government and Public Authorities	■	■	■	■	■	■	■		
Health		■	■	■		■	■		■
Maritime			■			■	■		
Nuclear						■	■		■
Public Safety	■		■			■	■		
Tourism			■			■	■		
Transportation		■	■			■	■	■	■
Smart Ecosystems		■	■			■	■		
Space						■	■		■
Supply Chain			■			■	■	■	

Table 35: JRC Sectors covered by SPARTA roadmap challenges

Chapter 12 Implications of COVID-19 on the Roadmap

The digital transformation has received a significant boost from the corona pandemic. Mobile working quickly became the new normal for millions of European citizens. Companies have also converted many of their business processes to digital processes within a very short time. As a result, local processes were shifted to cloud platforms rapidly. Consequently, the distance economy became the norm. In addition, due to bottlenecks in the provision of sufficient IT equipment at the employees' home offices, a large number of old IT systems with outdated software versions were used ad hoc to maintain production processes, business processes, logistics chains, communication, etc.

From an IT security perspective, these developments caused by the pandemic have very significant consequences. The number of vulnerabilities and the number of cyber-attacks on employees in the home office and on companies has risen sharply. The dependency on the availability of trustworthy software and hardware, as well as a reliable supply chain, has also increased significantly. In December 2020, Germany (BSI) and France (ANSSI) prepared a management report on the IT security situation caused by Covid 19[19]. Within their common assessment the two bodies stated, that it is necessary to foster development of various secured communication systems, to raise awareness with regards to supply chains issues, and to advocate life cycle management, security by design and by default on the part of IT providers.

In addition, and in some cases in-depth, to the above-mentioned report, we take up important issues in more detail from SPARTA's point of view and derive recommendations for action for the European Commission that could lead to a prioritization of activities within the Commission. SPARTA will use the results for the updated SPARTA roadmap in the next version. These aspects were drawn also inspired by the input from the SPARTA network collected through the aforementioned online questionnaire. Specifically, we asked SPARTA partners, associates & friends to rank the roadmap challenges with respect to the implications raised due the Covid-19 pandemic while providing a justification for their choice. Some of the most critical implications elaborated below have high impact on digital sovereignty which is underlined by their top ranking in Chapter 10.

1. Importance of trustworthy hardware and software for Europe:

Europe is dependent on third parties for many technical products and hardware components. The value chains, such as the production of chips, are global. Insights into which IT security requirements have been implemented in production and manufacturing are usually missing. However, Europe is heavily dependent on the secure functioning of its IT infrastructures.

Recommendations for the European Commission to prioritize activities

- Europe must be enabled to manufacture security-critical components such as trustworthy hardware chips itself to a large extent.
- In addition, Europe has to develop testable specifications for supplier components, to be able to control the whole development supply-chain.
- Europe must significantly expand its test and evaluation capacities in order to be able to automatically test components and their vendor parts, be it hardware or software. Testing tools and methods are required to assure security over the entire life cycle (i.e. also during operation).
- Europe must become a pioneer for technical standards.
- Europe must also develop internationally recognized certification schemes so that standards are adhered to in accordance with European testing and inspection procedures

[19] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DE-FR-Lagebild/de-fr_Lagebild_2020.pdf

and therefore with European values of openness, fairness and trustworthiness. Thus trust in the certification is built up.
- Europe must specifically build Open-source Communities for the development of trustworthy software and, among other things, develop technological alternatives for collaboration tools and video conference systems.

2. Importance of trustworthy data spaces for Europe:

The strong dependence of Europe on international cloud platforms became very clear. As a result of the distance economy, many companies were forced to use such platforms for the exchange of data in order to work together with their customers, business partners and suppliers. A large number of sensitive data are communicated and processed via these platforms and, in the future, new business processes will arise based on the data in the sense of a new data economy. This is of particular importance for the development of innovative applications of artificial intelligence, one of the most important innovation drivers for Europe in the coming years. For AI systems, training data and AI models are of great value and must be made usable in a safe and secure manner. Security here refers to both data protection and intellectual property issues. Those who master these data space have access to the basis for innovation processes in Europe.

Recommendations for the European Commission to prioritize activities

- Europe must invest massively in the development of protected data spaces. This includes both verifiably secure data spaces in the cloud and on edge devices through to secure sensors.

3. Importance of the human factor

The rapid increase in cyber-attacks due to the corona pandemic is largely due to the lack of security awareness, the lack of knowledge of users, but also to a lack of knowledge, as well as a lack of automated tooling, a lack of best practices and a lack of tailored trainings in companies. However, Europe does not only have to invest in improved education and training. Rather, Europe must also start fundamentally, as many users are overwhelmed by the complexity of the IT systems they use. Technical dependencies are often not understood. Therefore, users are not able to understand possible consequences of incorrect operation or wrongdoing. As a result, wrong decisions are often made with regard to security settings out of convenience, with fatal security related consequences.

Recommendations for the European Commission to prioritize activities

- Europe must invest in research to design user-friendly, resilient technology so that the possibility of errors caused by wrongdoing is reduced considerably.
- Technologies are required that also provide technical compensation so that compromised systems due e.g. to human errors can be recognized as such at an early stage, can automatically be cleaned up and thus safely integrated into company structures.
- New types of devices often do not have classic interaction options such as keyboards or screens. Secure user interfaces must be researched and developed for these devices.
- Europe must invest more in alternative and modern digital formats for security education and security training.

4. Importance of social media and Defence against fake information

During COVID-19 lockdowns, social media for information exchanges continued to gain in importance for many citizens. Important information is increasingly being displaced by targeted false information. With fake information people are being pushed into so-called information bubbles via global platforms that reach billions of people. This already showed serious consequences for democratic processes and democratic values. A central challenge for European research is to

develop binding frameworks for the future data and platform ecosystems that strike a balance between personal benefit, economic exploitation, democracy and data protection.

Recommendations for the European Commission to prioritize activities

- Europe must further develop its pioneering role in the data protection design of ICT systems. To this end, a focus should lie on research goals that develop privacy enhancing technologies, PETs.
- Business models have to be developed and it has to be shown that they are economically viable and at the same time work in a way that preserves data protection.
- AI systems are among the innovation drivers for Europe. Europe should become a pioneer in privacy preserving computing with and for AI.
- Digital media make it very easy to create deceptively real counterfeits and to bring them into circulation very quickly. Europe must invest heavily in the development of trustworthy detection technology and methods to automatically detect false information such as deepfakes in images, audio and video media.

In addition to detection, Europe should also develop processes and technologies with which valid information can be marked reliably and trustworthily. Such technologies must be developed in such a way that the classification of information is transparent and traceable. Advanced blockchain-based approaches could be an interesting starting point towards this goal. Europe should act as a pioneer and promote international standardization to promote a classification based on European values.

The COVID-19 pandemic underlines the necessity and prioritization of the central fields of action, which we already identified in Chapter 10 as fields with high priority. This includes trustworthy software and secure and fair AI. User-centric data governance plays an important role for building trustworthy data spaces. Hence, the high priority ranking is justified by the lessons learned from the pandemic as well. The human factor that has been shown of great importance during pandemic is addressed by education and training challenges within the SPARTA roadmap. This topic did not receive a high priority during the SPARTA-internal survey. Nevertheless, with respect to the lessons learned from the pandemic, this challenge should receive a higher priority than given in Chapter 10. Secure and fair AI is key to detect deep fakes and false information which aligns with the importance of the challenge for digital autonomy. In addition, trusted hardware and trustworthy supply chains are given a high priority due to the lessons learned from pandemic. This is currently missing in the ranking in Chapter 10, but we highly consider adding it in the next releases of the roadmap. Apart from that, we intend to sharpen the cybersecurity priorities in the next versions of the SPARTA roadmap by collecting input from broader audiences.

Chapter 13 Alignment of roadmaps

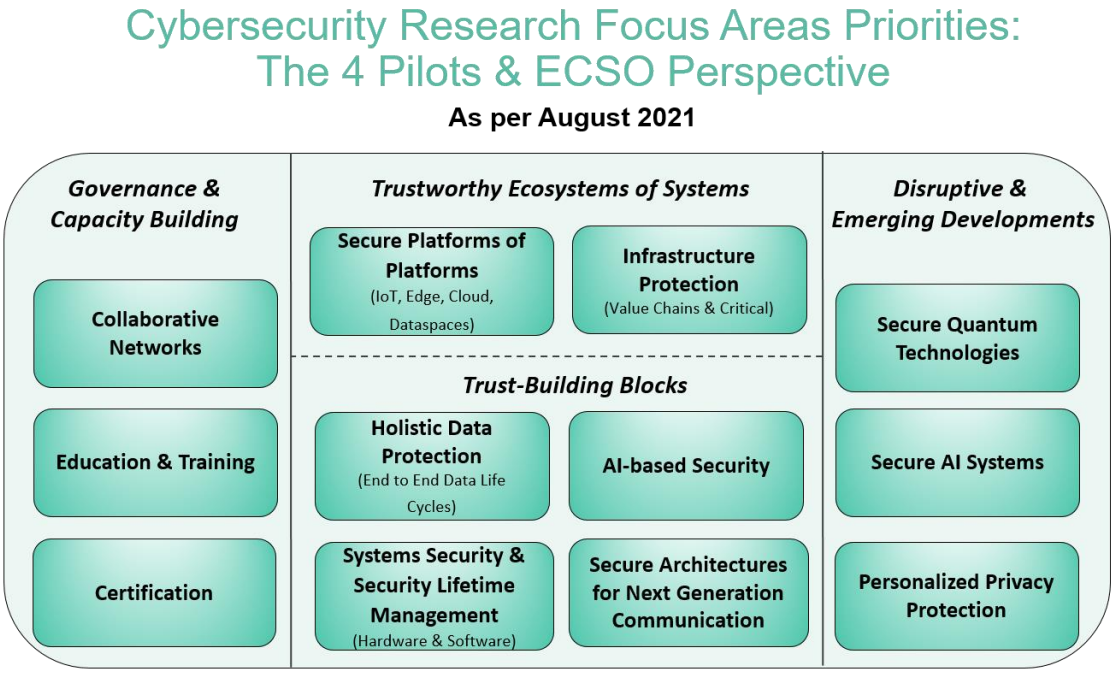
SPARTA has been in charge of coordinating a working group on prioritising cybersecurity challenges identified in the roadmaps and strategic research agendas of the four cybersecurity competence networks (Concordia, Cybersec4Eu, Echo, SPARTA) and ECSO. As part of its activities, the working group produced a document with a succinct description of a collection of challenges ("prioritised focus areas") that were identified by all partners as essential. The document provided input to work on drawing the EU Cybersecurity Atlas.

The Focus Group identified and discussed the following four areas:

1. Trust-building blocks.
2. Trustworthy eco-system of systems.
3. Governance and Capacity Building.
4. Disruptive and Emerging Developments.

Trust-building blocks concern software and hardware components used to engineer secure IT systems. This includes secure development methodologies, protection of data, the use of artificial intelligence for monitoring systems, and reliable next-generation communication technology. **Trustworthy eco-system of systems** is concerned with how to construct secure infra-structures from trusted components, acknowledging the variety of devices that take part in these networks. It also highlights the challenges arising from protecting the deployment of such infra-structures in supply-chains.

The first two areas are technological of nature, and concerns the research challenges that must be met in order to construct a secure IT infra-structure that can underpin the EU digital sovereignty. The third area on **Governance and Capacity Building** is concerned with the creation of European collaborative structures, with the strengthening of cybersecurity training and the building of a strong cybersecurity work force. It also addresses the essential question of how to construct a uniform certification process for the security of IT products that is both trust-building and cost-effective. The fourth area on **Disruptive and Emerging Developments** analyses the security challenges raised by some emerging technologies that are likely to the at the centre of IT infrastructures in the future. This includes most notably the security and reliability of applications based on artificial intelligence and, more prospectively, the security implications linked to emerging topic of quantum computing.



Each of these Cybersecurity Research Focus Areas Priorities are generally intertwined with each other.

13.1 Cybersecurity Research Focus Areas Priorities

In the following we describe the prioritised focus areas. The prioritised focus areas below are ranked in no particular order. They are seen as most notable yet non-exhaustive. As expected, these focus areas are generally intertwined with each other. The current prioritisation does not cover research priorities with respect to specific Sectors (Verticals). This is an additional dimension that will be addressed in the future.

13.2 Trust-Building Blocks

Using untrusted components in computer systems can easily compromise the security and privacy of the applications running within and the data they process. Thus, on the one hand, it is important to develop secure components, and on the other hand, we must ensure that the components we use from third parties are trustworthy and secure. To achieve that, more effort must be put into

(i) developing reliable software and hardware components that maintain their multilevel security requirements throughout their lifecycle,
(ii) building secure communication architectures for facilitating reliable massive data exchange between connected components,
(iii) protecting the data that these components store and process, and
(iv) leveraging AI-enhanced security mechanisms in order to withstand complex threats.

13.2.1 Systems Security and Security Lifetime Management (Hardware & Software)

Software is at the foundation of all digital technologies and, as such, at the core of the infrastructures, services, and products that the EU offers to its citizens. Current software development approaches prioritize fast deployment over security, which results in insecure applications. Thus, security engineering, both at the software and hardware levels, must be integrated in the development processes of today's complex systems. Moreover, a great portion of the software and hardware used in the EU is developed outside Europe, which is potentially untrusted as it may not comply with the

security requirements within the EU. To achieve digital sovereignty, Europe needs to be able to rely on software and hardware systems that can be verified and audited. This, in turn, requires methods, tools and engineers capable of conducting verification and security audits. In addition, the potential security gain of using open-source software and hardware amenable to analysis should be further explored. In addition, security and privacy regulations change frequently and software is subject to continuous update. As such, the compliance of IT systems cannot be assessed once and for all, hence methods and tooling to perform continuous assessments are needed.

- Trustworthy Certifiable (Open Source) Hardware
- Hardware & Software Security Engineering
- Software Analysis & Vulnerability Discovery & Dynamic Security Assessment
- Resilient Systems Design

13.2.2 Secure Architectures for Next Generation Communication

Next generation communication systems (including 5G, 6G, and beyond) aim to provide the smart Internet of everything offering a wide variety of applications. Although traditional communication systems have been studied for a long period, Next Generation Communication Systems introduce several novel and disruptive networking technologies, such Network Function Virtualization (NFV) and Software-Defined Networks (SDN), which in turn present several risks that need to be addressed. Security procedures in 5G networks need to be reshaped to cope with the new requirements of this paradigm, as the traditional solutions adopted in legacy networks are now outdated. The 5G ecosystem is bringing together many technologies expected to coexist in the same infrastructure. By making the Internet more transparent, accountable, and controllable at the network level, Responsible Internet seeks to increase trust and sovereignty for critical service providers and all types of users in general.

- Secure Next Generation Communication Systems
- Responsible Internet

13.2.3 Holistic Data Protection (End to End Data Life Cycles)

Recent advancements in digital technologies have led to an ever-increasing number of industries, critical infrastructures, households, and public administrations that store and process personal and otherwise sensitive data while connected to the internet. As a result, (cyber) attackers constantly find new ways to exfiltrate sensitive data, leading to a large amount of data breaches. To make matters worse, some organizations are not even aware of their data breaches until their data end up in the public domain or on the dark Web. To reduce the risk and potential impact of data breaches, data needs to be protected throughout its entire life cycle, from collection or generation over storage and processing to disposal. This includes to carefully consider, whether data is actually needed for the respective purpose and to equip stakeholders with instruments to make that assessment. Furthermore, user-centric privacy technology must be developed to put individuals back in control over their data, together with comprehensive identity and access management concepts to ensure that only legitimate users are able to access sensitive information. Finally, advanced digital forensics must support the identification of attackers and attack vectors in case of a breach, enabling developers and system administrators to further increase the security of their systems.

- User-Centric Data Governance: self-sovereign data governance
- Secure End to End Data Life Cycles: secure data acquisition, storage, transfer, processing, deletion
- Identity & Access Management
- Digital Forensics

13.2.4 AI-based Security

Artificial Intelligence (in particular Deep Learning and Machine Learning), together with advances in computing capacity, enable users to process very large amounts of data. As such, AI techniques have been successfully applied to tackle many cybersecurity problems via advanced methods for threat detection, prediction, and response. For example, AI mechanisms have the ability to combat the spread of digital fake assets, which are abused for misinformation and miseducation within our societies. The use of AI as a technology for building system monitoring techniques and anomaly detection should be developed further. At the same time, concerns have been raised over the security and stability of the AI algorithms used in cybersecurity applications. Thus, it is important to ensure that only certified, fair, and security-compliant AI algorithms are used to enhance cybersecurity. This is part of the specific Focus Area “Secure AI Systems” described below.

- AI-based Security Services e.g. predictive security, advanced anomaly and intrusion detection, system health checks
- Robust AI-based Fake Detection e.g. audio, video, images, speech

13.3 Trustworthy Ecosystems of Systems

Recent technological advances have led to the development of novel distributed computing platforms such as fog, edge, and cloud computing environments, that, when interconnected, build “systems of systems”. These advancements pave the way for novel ubiquitous applications, accessible from any computing device and from everywhere. As such, the stratified and static computing environments considered until now, in which applications run on mobile devices or cloud servers, have to evolve to accommodate novel dynamic computing paradigms. This computing model, however, introduces new security risks that threaten the critical and supply chain infrastructures, which power our societies and economies. Therefore, evolving computing frameworks must consider the interplay between edge, IoT, and cloud computing to understand how their interaction could stem evolving threat landscapes, and for dynamically managing the trust of distributed systems in a distributed yet secure manner.

13.3.1 Secure Platforms of Platforms (IoT, Edge, Cloud, Dataspaces)

The evolution of our interconnected society brings multiple layers of cloud, edge, and IoT platforms that continuously interact with each other. Yet this always-connected ecosystem populated with potentially vulnerable entities requires additional protection mechanisms that must manage their security and privacy through their lifecycle. The complexity of such interconnected environments underlines the need for proactive and automated approaches to the deployment of IoT devices in order to design a framework for the detection, analysis, and mitigation of cybersecurity attacks in IoT deployment. In addition, new requirements for availability and cloud capability at remote sites are needed to support today’s requirements (e.g., retail data analytics, network services, etc.) and tomorrow’s innovations (e.g., smart cities, AR/VR, etc.). The maturity, robustness, flexibility, and simplicity of cloud would thus need to be extended across multiple sites and networks in order to cope with evolving demands. Finally, integrating end-to-end security and user-centric privacy in platform of platforms requires research to solve key security threats and vulnerabilities all over the spectrum of cloud, to IoT devices and platforms.

- Cloud Infrastructures Vulnerabilities Mitigation
- Secure Integration of Untrusted IoT in Trusted Environments
- EU Multi-Cloud, Edge & IoT
- Trust & Security for Massive connected IoT Ecosystems & Lifecycle Management

13.3.2 Infrastructure Protection (Value Chains & Critical)

Critical infrastructures and their diverse supply chains have always been an attractive target for advanced attackers, mainly because their services and their distribution are essential for the well-being of society and its economy. Whether it is a physical infrastructure (e.g., a bridge, a road), a complex interconnected infrastructure (e.g., an energy distribution network, a physical/digital supply chain), or even the Internet itself, critical infrastructures together with their control systems can cause or enable major (sometimes irreparable) damage, if they are manipulated and/or cease to operate. As such, it is essential to devise novel security and privacy solutions that not only protect intertwined information technology assets in federated ecosystems, but also facilitate the secure and private collaboration between all physical and digital actors. Such solutions include not only traditional and advanced security measures, certification, and resilience, but also privacy-aware tools for sharing and processing Cyber Threat intelligence (CTI) information. In the development of these solutions, we need to consider key challenges related to the new ecosystems like industry 5.0, such as considering the human being as a key actor within the ecosystem, managing the interactions between multiple actors from different federated ecosystems using various technologies, and optimizing the use of resources at low cost, both technically and in terms of energy.

- Security across Value Chains: From Industry 5.0 to Supply Chains
- Critical Infrastructures Protection & Resilience
- Trusted Information Sharing & Collaborative Threat Intelligence Management

13.4 Governance & Capacity Building

The European Union has articulated the ambition to maintain its sovereignty and to become a global leader in the digital economy, guided by democratic values and resilient to cybersecurity threats. Research into designing governance structures will allow to create a comprehensive overview of the available capacities and their operation, to reinforce priority areas, and ultimately, to respond effectively to current and future cybersecurity challenges faced by Europe.

13.4.1 Collaborative Networks

European cybersecurity is a complex playing field of diverse stakeholders that continuously interact with each other. The growing diversity and sophistication of cyber threats requires the integration of a broad spectrum of competencies, human, technological and financial resources beyond the powers of a single organization or even a single country. The efficient and sustainable collaboration among variety of organisations builds on solid understanding of requirements, designing and implementing effective norms and models, and the supporting infrastructure.

- Governance of Collaborative Networks/Organisations

13.4.2 Education & Training

The growing demand for cybersecurity professionals and new levels of awareness of policy-makers and citizens calls for novel ways to educate and train individuals and teams. Individual academic and professional programs are already available at many universities and training institutions, but there is a lack of coordination and understanding, which courses and topics should be included in these programs to reflect the current trends on the job market. Additionally, in order to defend against cyberattacks, enterprises need to have a more concrete picture of their infrastructure and its specific security weaknesses, to improve their incident handling and response behaviour. As such, it is important to research more comprehensive frameworks of cybersecurity skills and competencies, new ways for design, use and re-use of training scenarios, monitoring and evaluation of knowledge and performance, federating cyber ranges and other supporting infrastructure. Additionally, cybersecurity skills frameworks should be constantly updated to keep up with the ever-evolving landscape of security threats. Moreover, investing in cybersecurity education and training towards sectoral and organizational characteristics can raise the security awareness of businesses and may

give them a tangible competitive advantage. Humans remain among the top factors leveraged by attackers to compromise the digital assets of companies and institutions. As security technologies improve, this trend is only expected to increase in the foreseeable future. Therefore, an integral education in cybersecurity competences is an ever-growing prerequisite for any enterprise to stand a chance against current and future cyberattacks.

- Education, Training, Cyber Ranges and Other Exercises

13.4.3 Certification

The increasing interconnectedness among systems and organizations calls for new levels of confidence that a particular device, product, system, process, or service are designed to and operate according to defined security policies. Cybersecurity certification has the ability to facilitate these guarantees, as it is able to formally attest or confirm certain security characteristics. Gaining cybersecurity certification for enterprises products or services can improve their level of security adding them confidence and thereby build blocks for a more competitive and resilient EU digital market. However, the conformity assessment process, which analyses the compliance to the respective cybersecurity certification goals is a complex evaluation process engaging risk assessment and requirements analysis, verification and testing procedures that needs to be further investigated and developed. Despite the existence of standardized approaches, such as ISO/IEC 18045 and the ETSI-TVRA methodology for IT security evaluation, there is a lack of standardized and widely used approaches indicating explicitly how to carry out the evaluation process for obtaining EU oriented cybersecurity certification (both to the assessor and to the entity that seeks certification). In addition, cybersecurity certification research should focus on how to ensure security throughout the lifetime of the design and development processes that constantly evolve to reduce the risk of harm from malicious exploitation facilitated by the collaboration between different stakeholders.

- Certification of Organisations, Products, Systems & Services, and Related Support

13.5 Disruptive & Emerging Developments

The continuous stream of technologies that emerge every year brings new developing opportunities but also a novel spectrum of cyberattacks. Ranging from Artificial Intelligence to Quantum Systems and Personalized Privacy, such technological breakthroughs are expected to play a pivotal role in our societies in the upcoming years. Thus, it is crucial to continuously examine emerging technological trends from a cybersecurity perspective, in order to understand the changing attack landscape and to design solutions that could thwart them.

13.5.1 Secure Quantum Technologies

Some of the main domains of quantum technologies, namely communication, computation, simulation, sensing and metrology, may produce transformative applications and have a real practical impact on our societies. Novel computing models are currently being explored that leverage hybrid quantum approaches for increased efficiency and applicability as opposed to traditional paradigms. As such, we need to make sure that quantum technologies will be integrated securely in novel quantum applications and that the emerging threats they introduce are understood prior to witnessing their consequences. Apart from enhancements in ubiquitous applications, quantum technologies also have the potential to impact modern security that we currently heavily rely on. While on the one hand, they may enable improved security of existing mechanisms, e.g., through quantum random number generation, they may also invalidate current security guarantees that rely on computationally hard problems. Thus, it is important to explore novel algorithms, such as post-quantum cryptography, that can preserve today’s security guarantees in post-quantum futures which can break the pillars of today’s security.

- Secure Quantum & Hybrid Computing [SPARTA SRIA, section 8.4]
- Secure Quantum Communications [SPARTA SRIA, section 8.4]
- Quantum Cryptography [SPARTA SRIA, section 8.4]
- Post-Quantum Futures

13.5.2 Secure AI Systems

Recent developments in Machine Learning (ML) have demonstrated that it can be used in a wide variety of applications: from impromptu interactions with humans to trading stocks. However, serious concerns have been raised about the security and reliability issues of machine learning models, which may make these models subject to new kinds of attacks. Such attacks can be efficiently applied to many application domains ranging from computer vision to natural language processing. For example, a self-driving car powered by AI could be manipulated to ignore speed limits or even worse to ignore the boundary of a dangerous cliff. To leverage the opportunities of ML technologies in a secure, safe, robust, and trustworthy way, available technologies should be advanced by substantial investments to eventually allow for secure and safe AI systems, that can be certified as such and are explainable, despite complex boundary conditions and, therefore, to improve scalability and fairness. These technologies are most likely to help in future to overcome the trade-off between complex models with high accuracy and secure models that can be explained easily.

- Secure Certifiable AI Systems (including certifying AI as a trust-building block)

13.5.3 Personalized Privacy Protection

The digital transformation is encouraging the emergence of new scenarios where a large volume of data is shared and employed to enhance common services. Despite its advantages, this technological evolution is also bringing new security and privacy challenges related to the treatment of such data, especially in case of personal information, where an improper use could violate people's privacy. Also different Privacy Enhancing Technologies need to be explored in order to protect and facilitate privacy-respecting sharing personal data, such as secure multi-party computation or fully-homomorphic encryption, considering that data privacy is a task that requires more than just applying a predefined set of techniques or technologies. Given the rapid digital transformation, continuous research activities are focusing on, e.g., scalability, long-term security, and flexibility of such technologies. However, privacy also has more requirements, such as legal regulations and individual privacy preferences. Therefore, every system that is handling sensitive data should also collect and record the privacy preferences of the individual to whom the data refers, also known as data subjects.

- Advanced Privacy Protection Requirements, stemming e.g. from social media technologies, precision medicine applications.

Chapter 14 Conclusion

The SPARTA roadmap identifies, analyses and describes **key challenges in cybersecurity** that must be solved in order to achieve SPARTA's mission to strengthen **EU's digital sovereignty**. The roadmap addresses technological, educational, and certification-related aspects of the challenges, and proposes a time-line for their solution.

The agile and open **process** for achieving the present roadmap is an important experience gained from the work on the SPARTA roadmap. The roadmap has been based on several sources of input. An important initial input was the set of over 60 seed challenges collected from the SPARTA partners and the four programs that were constructed out of those challenges. Another basis was the overview of the existing national and international roadmaps, as well as the European JRC taxonomy. Based on all this information, the roadmap committee and SPARTA partners in the roadmap work package analysed a series of long-term challenges (Program Challenges and Emerging Challenges) and described them using the roadmap template developed for this purpose. A significant part of these challenges arose from collaboration with SPARTA Program Leaders and Activity Leaders of other work packages. These long-term challenges constitute the pillars of the SPARTA roadmap for cybersecurity research and innovation in Europe.

The extensive **description of long-term challenges** encompasses multiple aspects. They start with a description of the problem, the final goal that should be strived for, and the current state at European and international level. The challenges are analysed from several angles: in addition to the research aspects, they are also analysed in terms of the industrial demand, social aspects, as well as the concrete benefits for the EU from tackling this challenge. This is complemented a brief SWOT analysis in order to better characterize the challenge. Moreover, each challenge is related to the JRC taxonomy and the emerging technologies that were identified as relevant. For each challenge a tentative timeline, is suggested, envisioning the path from the status quo to the final solution. This should help as a guide for SPARTA Programs and research and innovation activities in Europe in general. A part of the SPARTA roadmap is dedicated to long-term challenges that were either previously put forward at the European level or identified during SPARTA by the roadmap committee. These emerging challenges have been described at a higher level which is still sufficiently detailed to provide a basis for their future refinement into full-fledged SPARTA challenges.

The roadmap proposes a first step towards a **prioritization** of the roadmap challenges that gives an overview on the most critical areas that the EU should concentrate on for moving towards digital autonomy. The prioritization was achieved by synthesizing input collected on the SPARTA roadmap via an online survey. The process used to produce this ordering is scalable and should be able to serve as a mechanism for collecting feed-back from more cybersecurity communities, thereby obtaining a better inclusion of network associates and other network partners across the EU. Moreover, the SPARTA roadmap presents its favourable view on the open-source philosophy and highlights the cybersecurity benefits of open-source software and hardware for achieving digital autonomy in the EU. The roadmap document also identifies critical cybersecurity risks implied by the COVID-19 pandemic and proposes a collection of recommendations for how to mitigate them.

Chapter 15 List of Abbreviations

Abbreviation	Translation
II	Intelligent Infrastructure
IoT	Internet of Things
JRC	Joint Research Centre
PET	Privacy Enhancing Technologies
SME	Small and Medium-sized Enterprises
SWOT	Strengths, Weaknesses, Opportunities, and Threats
WP	Work Package

Chapter 16 References

[1] IEC 62443, Industrial automation and control systems security/ Network and system security for industrial process measurement and control.

[2] SAE J3061, “Cybersecurity Guidebook for Cyber-Physical Vehicle Systems”, http://standards.sae.org/wip/j3061/, January 2016

[3] International Organization for Standardization (ISO), ISO 26262 "Road vehicles – Functional safety", 2011.

[4] AMASS Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems, https://www.amass-ecsel.eu/

[5] EMC2, Embedded Multi-Core systems for Mixed Criticality applications in dynamic and changeable real-time environments, https://www.artemis-emc2.eu/

[6] MERGE, Multi-Concerns Interactions System Engineering http://www.merge-project.eu/

[7] C. Schmittner, Z. Ma and P. Smith, “FMVEA for Safety and Security Analysis of Intelligent and Cooperative Vehicles“, FMVEA for Safety and Security Analysis of Intelligent and Cooperative Vehicles", Computer Safety, Reliability, and Security: SAFECOMP, Florence, Italy, September 8-9, 2014