D3.1

Initial SPARTA SRIA (Roadmap v0.1)

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 / D3.1 / V1.0
Work package contributing to the deliverable	WP3
Due date	July 2019 – M06
Actual submission date	31st July, 2019

Responsible organisation	TUM, INRIA
Editor	Sergej Proskurin
Dissemination level	PU
Revision	V1.0

Abstract	Initial roadmap for SPARTA based on identified and discussed dimensions and taxonomies. It contains information from SPARTA Programs and new identified challenges.
Keywords	Roadmap

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

Editor

Sergej Proskurin (TUM)

Contributors (ordered according to beneficiary numbers)

Philippe Massonet (CETIC)

Jan Hajný (BUT)

Bojan Kolosnjaji, Mohammad Norouzian, Claudia Eckert (TUM)

Hervé Debar (IMT)

Ludovic Me, Thomas Jensen (INRIA)

Artsiom Yautsiukhin (CNR)

Evaldas Bruze (L3CE)

Michał Choraś, Marek Pawlicki (ITTI)

Reviewers (ordered according to beneficiary numbers)

Thibaud Antignac, Florent Kirchner, Augustin Lemesle (CEA)

Artsiom Yautsiukhin (CNR)

Disclaimer

Executive Summary

This deliverable contains the initial SPARTA roadmap. The roadmap comprises challenges that were identified in collaboration with SPARTA partners. The main challenges form the four main SPARTA Program challenges: T-SHARK, CAPE, HAII-T, and SAFAIR. Further challenges are grouped into transversal challenges that mainly focus on “cybersecurity education and training” as well as “certification organization and support” challenges and are covered by other SPARTA work packages. The final set of challenges included in the SPARTA roadmap comprises emerging challenges; the SPARTA consortium members believe that these emerging challenges will become relevant for the EU in the future. The roadmap summarizes these challenges in a timeline that defines short-, mid-, and long-term goals that are required to complete the challenges.

The comprehensive approach of creating the SPARTA roadmap involves not only research topics, but also topics that focus on certification and education. Furthermore, in addition to technology, we take into account industrial, social, and economic aspects. We make special consideration of benefits for the EU and its strategic autonomy. The first steps towards creating the roadmap incorporated a thorough collection of more than 60 seed challenges that became the basis for the four SPARTA Programs. Each Program further subdivides the crystallized goals into a set of sub-challenges, some of them being addressed in SPARTA. We further include long-term challenges that align the programs with aspects of education and certification. Moreover, we isolated long-term challenges for education and training as well as certification and incorporate those within the initial roadmap.

During the creation of this initial roadmap, we took into consideration the already existing roadmapping 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. For instance, research domains, including “theoretical foundations”, “identity and access management”, and “network and distributed systems” were covered only partially or not at all by the EU states represented among SPARTA partners. The same applies to the technologies covering “operating systems”, “pervasive systems”, “vehicular systems”, and “hardware technology”. Finally, the sectors regarding “audiovisual and media”, “digital infrastructure”, “maritime”, “nuclear”, “public safety”, and “supply chain” as well show a lack of consideration. These findings help us to identify topics that were collectively disregarded in the past and thus potentially open up new directions.

Based on this existing information and our previously described approach, we created a template for contribution to the roadmap. We use this template that describes the identified long-term challenges in cooperation with leaders of Programs and certification and education work packages. Finally, we used the information from the templates to create a visualized timeline that indicates how technological development affects the education and certification aspects and vice versa.

Finally, a comparison of our roadmap to the JRC taxonomy shows that the challenges that we defined cover most of the crucial technologies, vertical sectors, and research domains. Our roadmap shows that we can leverage the strength of EU countries in a wide range of expertise and we intend to turn challenges into opportunities for development and the increase of the EU strategic autonomy.

Table of Content

List of Figures

List of Tables

Chapter 1 Introduction

This document represents the efforts of partners in Working Package 3 (WP3) to establish an initial roadmap for research and innovation, leveraging the expertise of the consortium in technology, education and certification, corresponding to the goal of task 3.1 – Initial Roadmap Design. 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. Although the general view over existing roadmaps and identification of new challenges are part of tasks 3.2 and 3.3, we leverage their early results to make a more well-rounded approach for this initial roadmap.

We begin by explaining the reasoning behind the creation of our roadmap, relating it to existing taxonomies and roadmapping principles in Chapter 2. In Chapter 3, we analyze the landscape of national and international roadmapping activities in European countries represented in SPARTA. Also, we relate the previously done roadmapping 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 taking into account 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. Then, Chapter 9 describes the relationship between the long-term challenges and the JRC taxonomy. Finally, Chapter 10 concludes with an outlook on future work on this comprehensive roadmap.

Chapter 2 The SPARTA Approach

The SPARTA consortium will establish a strategic research and innovation roadmap that stimulates the development and deployment of key technologies in cybersecurity to retain digital sovereignty and autonomy of the European industries and governments to increase trust in products, services and infrastructures of our future society will depend on. During the phase of proposal writing, the project partners have already collected more than 60 seed challenges. Consortium members, belonging to different organizations, have reviewed these seed challenges and designed four research programs (WP 4, 5, 6, 7). The Embryo Roadmap has now been converted into the present initial SPARTA roadmap. The SPARTA roadmap serves as both the common ground for the alignment of research, education and certification priorities of the European Cybersecurity Competence Network (in the sense of an agenda, and reaching beyond the project duration) and the guideline for successful completion of the project (in terms of targets to be achieved within the project duration). For the initial roadmap, it has been decided to put the focus not only on new technologies but also to consider industrial, societal and economic directions. The initial roadmap considers the goals of the four SPARTA programs T-SHARK, CAPE, HAII-T, and SAFAIR as well as three SPARTA long-term challenges. These long-term challenges cover emerging goals focusing on privacy, autonomous security, and trustworthy software. Each long-term challenge is described through different dimensions including the coherent and comprehensive JRC taxonomy for categorizing EU cybersecurity competences.

For creating the SPARTA roadmap, we take into account existing roadmaps (e.g., ECSO roadmap) in order to identify opportunities for improvement in exiting solutions. The idea is to establish a roadmap that will be maintained, meaning regularly updated, to reflect on changes and most importantly, progress made within the SPARTA project and beyond. These aspects will make the SPARTA roadmap a useful tool to make strategic decisions. An essential aspect of the roadmap maintenance will be the interaction with the end-users through inputs collected during the monthly SPARTA workshops.

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 JRC's taxonomy for cybersecurity R&I topics. Such an approach allows us to find the topics, which have already got 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 is not of top priorities, 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 roadmapping 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 sum, we conclude that the SPARTA's partners have excellent expertise and are heterogeneous enough to select the best set of materials for the analysis.

3.1 Analyzed documents

We have selected the following documents to be analyzed 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
- Lithuania: National Cyber Security Strategy[6] (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
[6] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Lithuania_Cyber_Security_Strategy.pdf

- 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 analyzed 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 use the recent JRC taxonomy[18] for cybersecurity research. The taxonomy is comprehensive enough and is focused on research and innovation in cybersecurity.

The JRC's taxonomy defines three vectors 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.

---

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/JRC111441/taxonomy_final.pdf

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;
- Theoretical Foundations;
- Trust Management, Assurance, and Accountability.

The Applications and Technologies vector contains the following topics:

- Artificial intelligence;
- Big Data;
- Blockchain and Distributed Ledger Technology (DLT);
- Cloud and Virtualisation;
- Embedded Systems;
- Hardware technology (RFID, chips, sensors, routers, etc.)
- Industrial Control Systems (e.g., SCADA);
- Information Systems;
- Internet of Things;
- Mobile Devices;
- Operating Systems
- Pervasive systems
- Quantum Technologies
- Robotics;
- Satellite systems and applications;
- Supply Chain;
- Vehicular systems

The following Sectors are considered by JRC:

- Audiovisual and media
- Defense
- Digital Infrastructure
- Energy
- Financial
- Government and public authorities
- Health
- Maritime
- Nuclear
- Public safety
- Tourism
- Transportation
- Smart ecosystems
- Space
- Supply Chain

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 analyzed 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 colors (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 color. 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	Total
	2013	**2013**	**2015**	**2015**	**2016**	**2017**	**2018**	**2018**	**2018**	**2019**	**2019**	**2019**	
Assurance, Audit, and Certification	■			■	■	■	■			■		■	7
Cryptology				■	■		■				■		4
Data Security and Privacy		■		■	■		■		■		■		6
Education and Training	■	■	■		■	■	■	■	■	■	■		10
Operational Incident Handling and Digital Forensics	■		■			■	■	■	■	■	■	■	9
Human Aspects				■	■						■		3
Identity and Access Management											■		1
Security Management and Governance	■	■	■		■	■	■	■	■	■	■	■	11
Network and distributed Systems				■	■	■							3
Software and Hardware Security engineering	■	■				■	■		■				5
Security Measurements	■								■	■			3
Legal Aspects		■	■					■		■	■		5
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.

- Security Management and Governance
- Education and Training
- Operational Incident Handling and Digital Forensics
- Assurance, Audit, and Certification
- Data Security and Privacy

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. A similar observation could be made about *Assurance, Audit and Certification.* Finally, we should note that we see no notable change in the coverage of the six years.

	Spain Ind.	Austria	Czech	Germany	Spain	Poland	Italy	Lithuania	Luxemburg	Greece	France INRIA	France	Total
	2013	**2013**	**2015**	**2015**	**2016**	**2017**	**2018**	**2018**	**2018**	**2019**	**2019**	**2019**	
Artificial intelligence;							■			■	■	■	4
Big Data;			■	■	■				■				4
Blockchain and Distributed Ledger Technology (DLT);							■				■		2
Cloud and Virtualisation;					■		■		■		■		4
Embedded Systems;					■				■			■	3
Hardware technology (RFID, chips, sensors, routers, etc.)													0
Industrial Control Systems (e.g. SCADA);			■	■	■		■		■		■		6
Information Systems;											■		1
Internet of Things;			■		■		■				■		4
Mobile Devices;					■								1
Operating Systems													0
Pervasive systems													0
Quantum Technologies;				■			■						2
Robotics;							■				■		2
Satellite systems and applications;					■								1
Supply Chain;						■					■		2
Vehicular systems													0

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

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

- Industrial Control Systems
- Artificial intelligence
- Big Data
- Cloud and Virtualisation
- Internet of Things

Again, we see that the two topics of SPARTA's pilots (Artificial Intelligence and IoT are among the highest). From this analysis, we see that some topics gain popularity: e.g., Artificial intelligence. We also may note that Blockchain and Distributed Ledger Technology, Robotics, and Supply Chain have a similar attitude.

	Spain Ind.	Austria	Czech	Germany	Spain	Poland	Italy	Lithuania	Luxemburg	Greece	France INRIA	France	Total
	2013	2013	2015	2015	2016	2017	2018	2018	2018	2019	2019	2019	
Audiovisual and media													0
Defence									■				1
Digital Infrastructure													0
Energy					■		■		■	■			4
Financial					■		■		■				3
Government and public authorities							■						1
Health				■	■				■	■	■		5
Maritime													0
Nuclear													0
Public safety													0
Tourism							■						1
Transportation				■	■		■		■				4
Smart ecosystems					■								1
Space									■				1
Supply Chain													0

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

As for the Sectors, then the most cited are:

- Healthcare
- Energy
- Transportation
- Financial

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).

3.3.2 European roadmaps

European roadmaps we analyze 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 to *Data Security and Privacy* and devoting much less attention to the *Operational Incident Handling* and *Legal aspects*. Although, it is not entirely clear out of the data we have at hand, but we may see a slight shift to the right of documents mentioning *Operational Incident Handling,* which may be explained by more interest devoted to the topic in the recent years. We may 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. We also should note that the Aegis project has a similar comment from experts about their priorities.

	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 Thing
- 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 modeling. 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 is the top one in our analysis and it covers many important aspects of cybersecurity; thus, it is not surprising to see many subtopics, which have got much attention.

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 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 has started with four programs that are summarized in the initial SPARTA roadmap together with goals related to education and certification. Further, our idea is to go beyond the four programs to identify emerging long-term challenges that are not yet covered by the four programs. In fact, the roadmap committee, considering the feedback from a diverse set of stakeholders, identified relevant topics forming final strategic goals to be included in a SPARTA roadmap challenge template. This template is used to describe long-term challenges and possible paths to their completion in Chapter 5. This template comprises three tables that are described in more detail in the following. This template represents a framework that 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. In an upcoming phase of the roadmapping process, it is planned to use visualization techniques of our German SPARTA partner (University of Konstanz) to provide a more comprehensive representation of our 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 which describe the addressed challenge. For this, we have to consider 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 emerging technologies that could either benefit from the expected outcome of the challenge or can influence research activities can be linked to the particular challenge, we also state them in a separate field.

Before introducing in detail the subgoals of each challenge, a figure gives a high-level overview of the challenge timeline. In particular, we create a timeline, these figures depict 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 kinds, 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*, we establish a direct connection to this frame of reference. Furthermore, we add a dimension called *regulation*, which is for instance, also present in the CAMINO roadmap[19].

The descriptions of challenges and timelines reflect the current vision of members of the SPARTA

Consortium. As this is the initial version of the roadmap, it still contains some fields that are yet to be completed in the future, during the roadmap update cycle. However, it is already comprehensive enough to enable useful conclusions.

[19] http://www.fp7-camino.eu/

Chapter 5 Initial Sparta Roadmap

This chapter summarizes the roadmap challenges, described in Chapter 6, Chapter 7, and Chapter 8, in a unified timeline of the initial 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. Besides, the timeline further includes emerging challenges that base upon the 60 initial challenges and have been identified by program partners. 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 pursued by SPARTA; this detailed view excludes, e.g., emerging challenges that go beyond SPARTA. Further, Figure 2 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 pilot are shown for each year and at the end, the final goal is displayed.

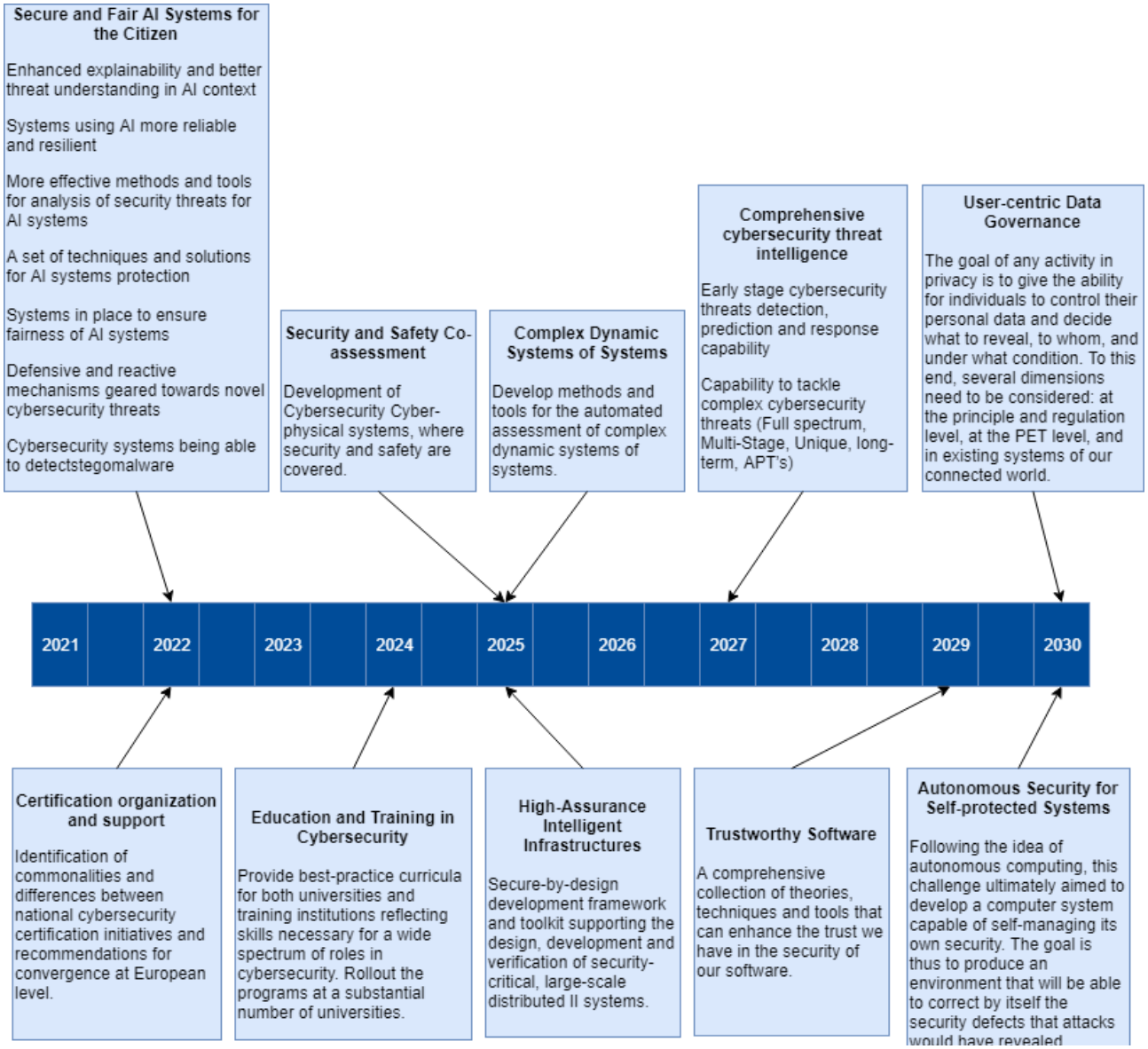

Figure 1: Roadmap with the final goals of solving the identified challenges

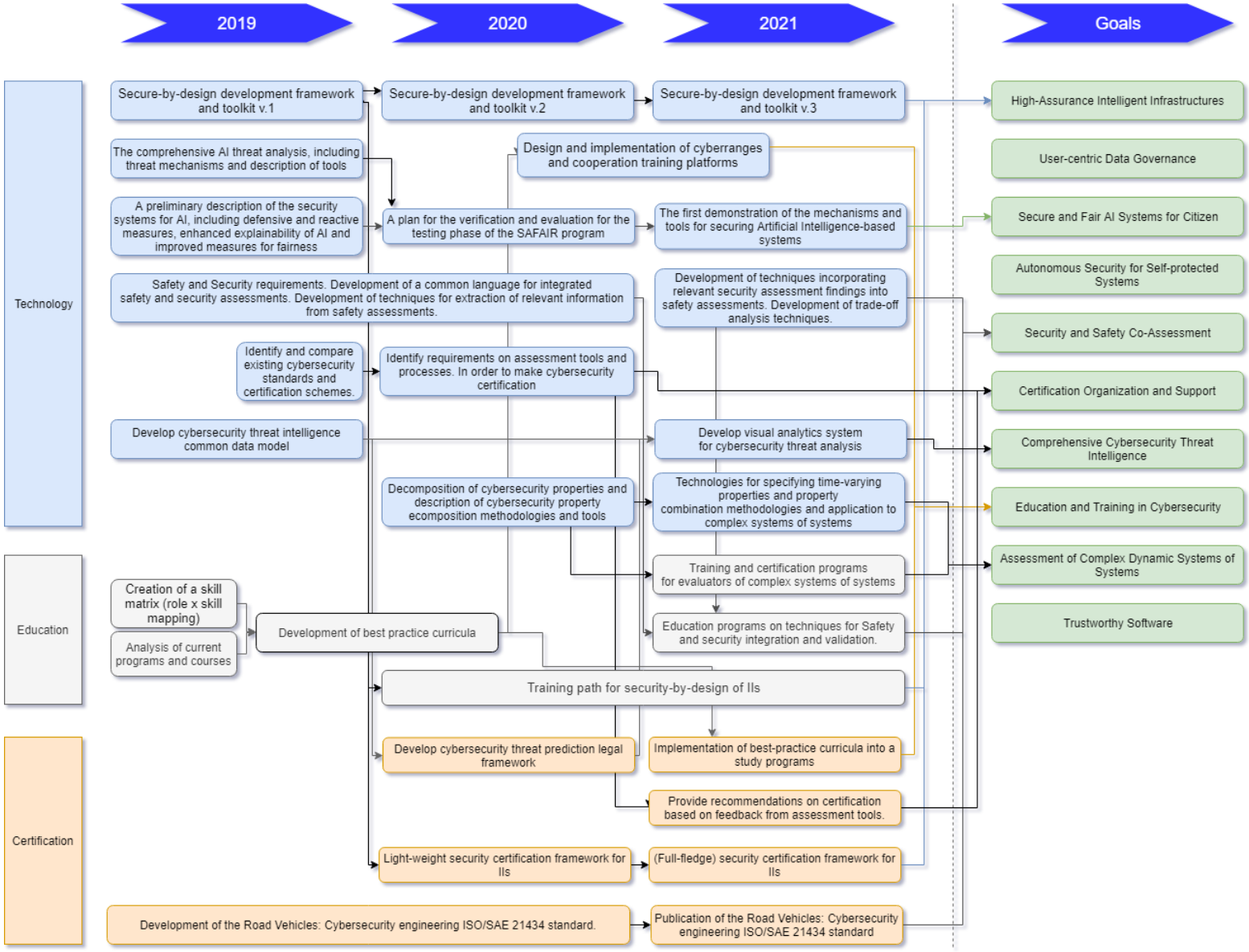

Figure 2: Timeline of stages for technology, education and certification

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 requires 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 a more and more significant role in cyber threats therefore
- **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 is 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,

rises lots of regulatory questions and demands: how to define the threat, how to measure it, what privacy, ethical and other standards should be applied in order to maintain the balance between enforcement and individual rights.
- **Legal:** tackling the cyber threats – what 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 originates 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 academical 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

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)
- The 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 capability 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):

- Defense, 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)

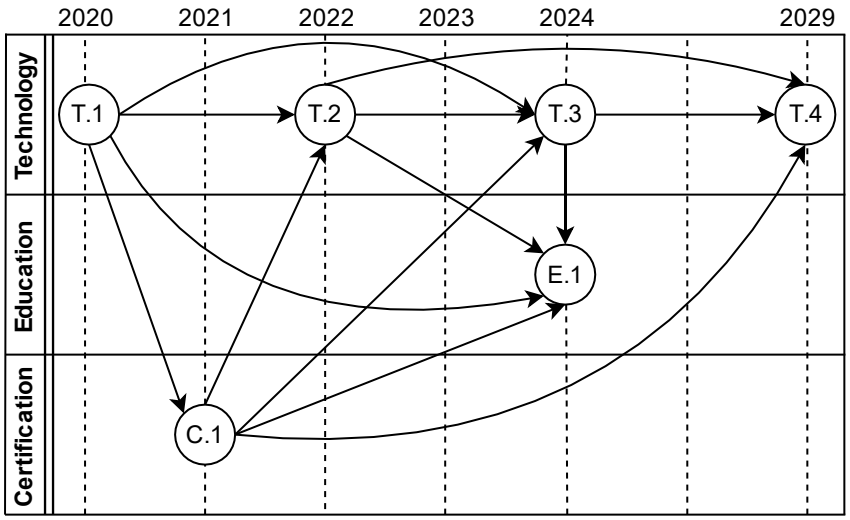

Figure 3: Timeline for the expected completion of subgoals for Comprehensive Cybersecurity Threat Intelligence (from T-SHARK)

Stage/Dimension	Sector (JRC)	Domain (JRC)	Regulation
T1	Public Safety, Government and Public Authorities, Defense, 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, Defense, 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 is 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, Defense, 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, for the large scale and critical incidents to have reactive organization of cybersecurity function is not enough and sometimes even too late. Therefore, for this subset of cybersecurity topic, preventive organization of the cybersecurity function is required, requiring 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 likehood 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, Defense, 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>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 the once 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, those 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 treats) 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><table>
<tr><td>Public Safety, Government and Public Authorities, Defense, 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):

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></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, Defense, 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. One of the most remarkable standards is IEC 62443 [1] for industrial automation, which gives guidance on how security threats for safety-critical control systems shall be treated. Another example is the SAE J3061 [2] standard, which defines a safety and security interaction point approach corresponding to the automotive functional safety standard ISO 26262 [3].

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)

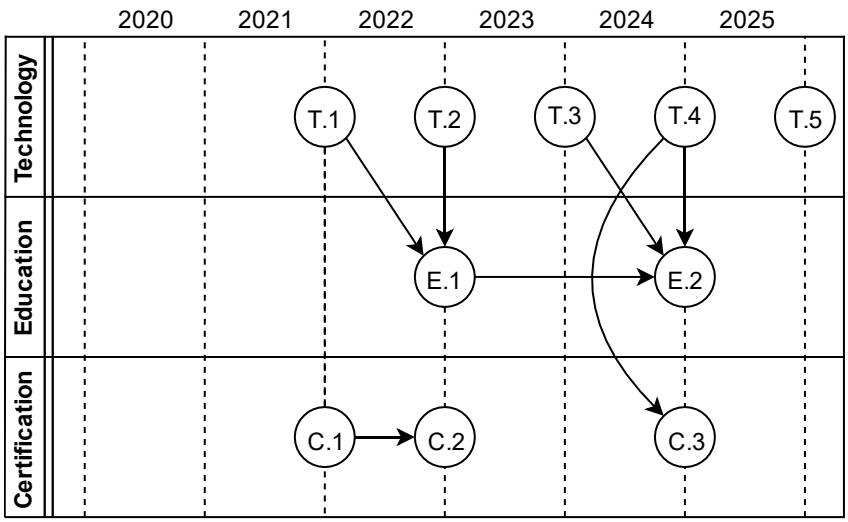

Figure 4: Timeline for the expected completion of subgoals for Security and Safety Co-Assessment (from CAPE)

Stage/Dimension *Tx for Technology* *Ex for Education* *Cx for certification*	**Sector (JRC)**	**Domain (JRC)**	**Regulation**
T1	Energy, Financial, Government and Public Authorities, heath, 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, heath, Transportation, Smart ecosystems.	Education and Training	
	Description (incl. obstacles): Development of techniques incorporating relevant security assessment findings into safety assessments. Development of trade-off analysis techniques.		

<table>
<tr><td rowspan="2">T3</td><td>Energy, Financial, Government and Public Authorities, heath, 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, heath, 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. Incremental methods, however, still shall guarantee the safety and security of the system that is updated.</td></tr>
</table>

<table>
<tr><td></td><td colspan="3">Obstacles: The degree of incrementality may not enable techniques to re-use parts of the assessments.</td></tr>
<tr><td rowspan="2">T5</td><td>Energy, Financial, Government and Public Authorities, heath, 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):
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.</td></tr>
<tr><td rowspan="2">E1</td><td>Energy, Financial, Government and Public Authorities, heath, Transportation, Smart ecosystems.</td><td></td><td></td></tr>
<tr><td colspan="3">Description (incl. obstacles):
Education programs based on Safety and Security assessment.</td></tr>
<tr><td>E2</td><td>Energy, Financial, Government and Public Authorities, heath, Transportation, Smart ecosystems.</td><td></td><td></td></tr>
</table>

	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): Development 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): Publication 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): Development a methodology to assess safety and cybersecurity of systems.		

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 thus to 1) define and publish the appropriate cybersecurity properties, 2) assess that these properties are met by increasingly complex and dynamic systems and services, and finally 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 behavior
- 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)

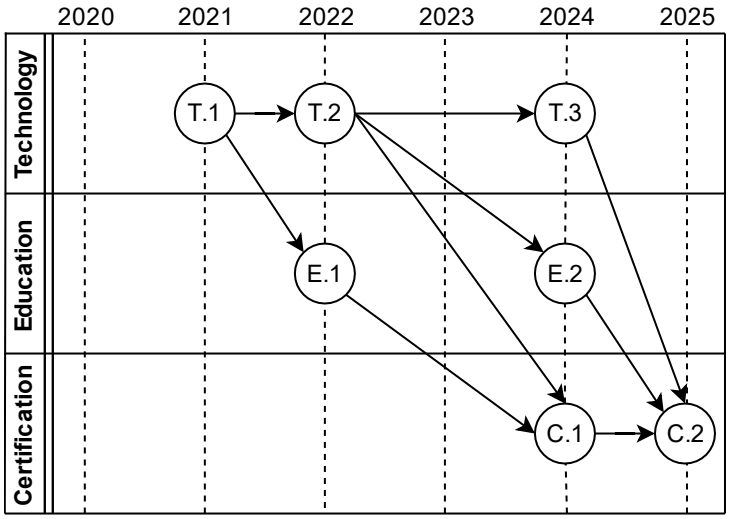

Figure 5: Timeline for expected completion of subgoals for Complex Dynamic Systems of Systems (from CAPE)

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		

<table>
<tr><td></td><td colspan="3">complex interactions, which will have an impact on global cybersecurity properties</td></tr>
<tr><td rowspan="2">T2</td><td>All sectors</td><td>Assurance, Audit and Certification</td><td>CC, SOG-IS</td></tr>
<tr><td colspan="3">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.</td></tr>
<tr><td rowspan="2">T3</td><td>All sectors</td><td>Assurance, Audit and Certification</td><td>CC, SOG-IS</td></tr>
<tr><td colspan="3">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.</td></tr>
</table>

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 more and 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, domotics, 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)

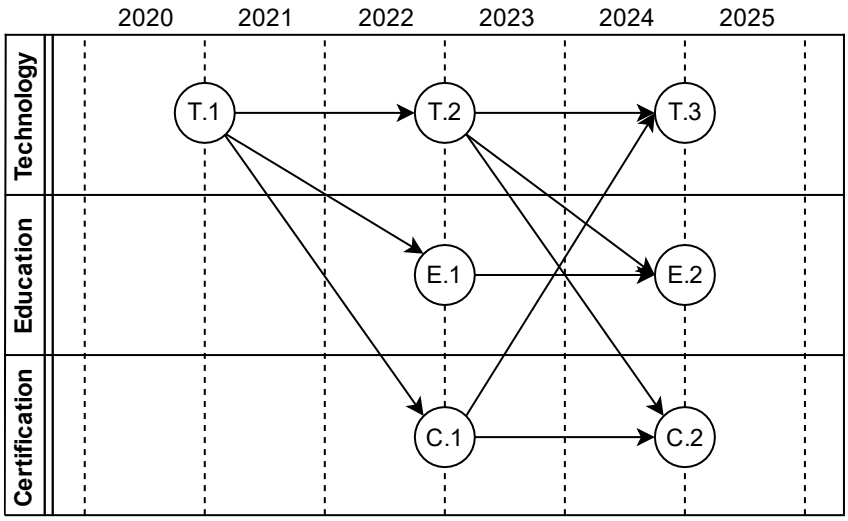

Figure 6: Timeline for expected completion of subgoals for High-Assurance Intelligent Infrastructures (from HAII-T)

Stage/Dimension *Tx for Technology* *Ex for Education* *Cx for certification*	**Sector (JRC)**	**Domain (JRC)**	**Regulation**
T1	Equivalent to Table 11	Equivalent to Table 11	
	Description (incl. obstacles): HAII-T secure-by-design development framework and toolkit v.1 ...		
T2	Equivalent to Table 11	Equivalent to Table 11	
	Description (incl. obstacles): HAII-T secure-by-design development framework and toolkit v.2 ...		
T3	Equivalent to Table 11	Equivalent to Table 11	
	Description (incl. obstacles): HAII-T secure-by-design development framework and toolkit v.3 …		
E1	Equivalent to Table 11	Equivalent to Table 11	
	Description (incl. obstacles): HAII-T training path for security-by-design of IIs (target: designers and developers of IIs)		
E2	Equivalent to Table 11	Equivalent to Table 11	
	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)		
C1	Equivalent to Table 11	Equivalent to Table 11	
	Description (incl. obstacles): HAII-T light-weight security certification framework for IIs		
C2	Equivalent to Table 11	Equivalent to Table 11	
	Description (incl. obstacles): HAII-T (full-fledge) security certification framework for IIs		

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 individual 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.

Final goal:

- Enhanced explainability and better threat understanding in AI context
- Systems using AI more reliable and resilient
- 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 educational 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.
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 Foundation, 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

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

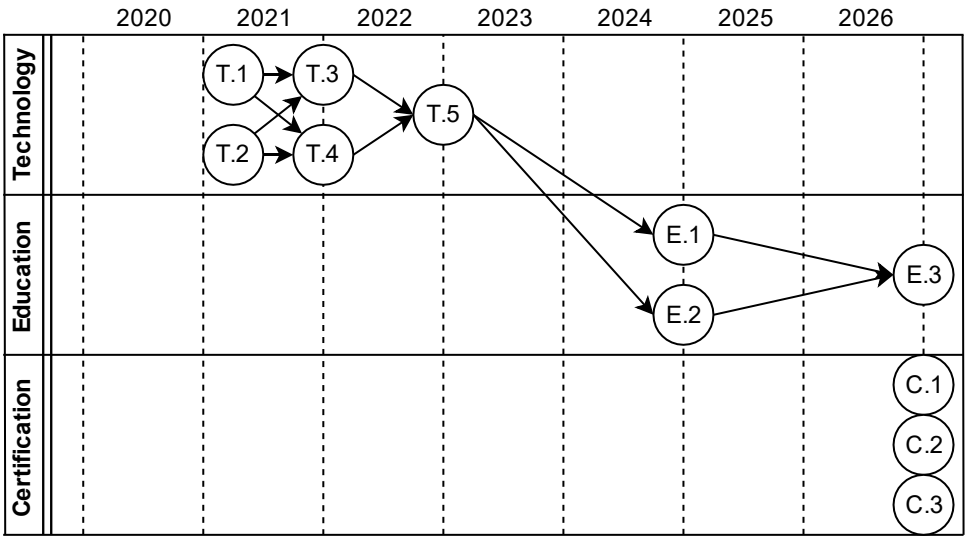

Figure 7: Timeline for expected completion of subgoals for Secure and Fair AI Systems for Citizen (from SAFAIR)

Stage/Dimension *Tx for Technology* *Ex for Education* *Cx for certification*	**Sector (JRC)**	**Domain (JRC)**	**Regulation**
T1	All sectors	Cybersecurity	
	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	
	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	
	Description (incl. obstacles): A plan for the verification and evaluation for the testing phase of the SAFAIR program		

T4	All sectors	Cybersecurity	
	Description (incl. obstacles): The first demonstration of the mechanisms and tools for securing Artificial Intelligence-based systems		
T5	All sectors	Cybersecurity	
	Description (incl. obstacles): The final version of security mechanisms and tools for AI systems		
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, Cybersecurity ranges, Cybersecurity education methodology, Certification Programmes.
Sector (JRC Taxonomy): Government and Public Authorities, Publishing, Internet
Relation to Emerging Technologies: Cyberranges, Gamification

Table 17: General information for Education and Training in Cybersecurity

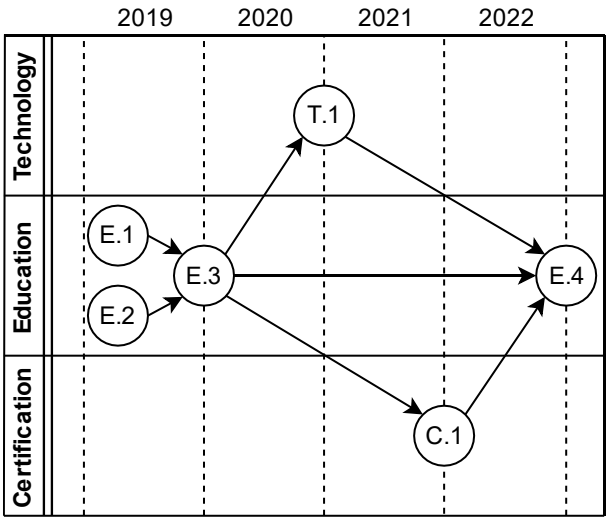

Figure 8: Timeline for expected completion of subgoals for Education and Training in Cybersecurity

Stage/Dimension *Tx for Technology* *Ex for Education* *Cx for certification*	**Sector (JRC)**	**Domain (JRC)**	**Regulation**
T1	Equivalent to Table 17**Fehler! Verweisquelle konnte nicht gefunden werden.**	Cybersecurity education, Cybersecurity exercises, Cybersecurity 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 analyze 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.

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: Artificial intelligence can be used by 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 analyzing 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

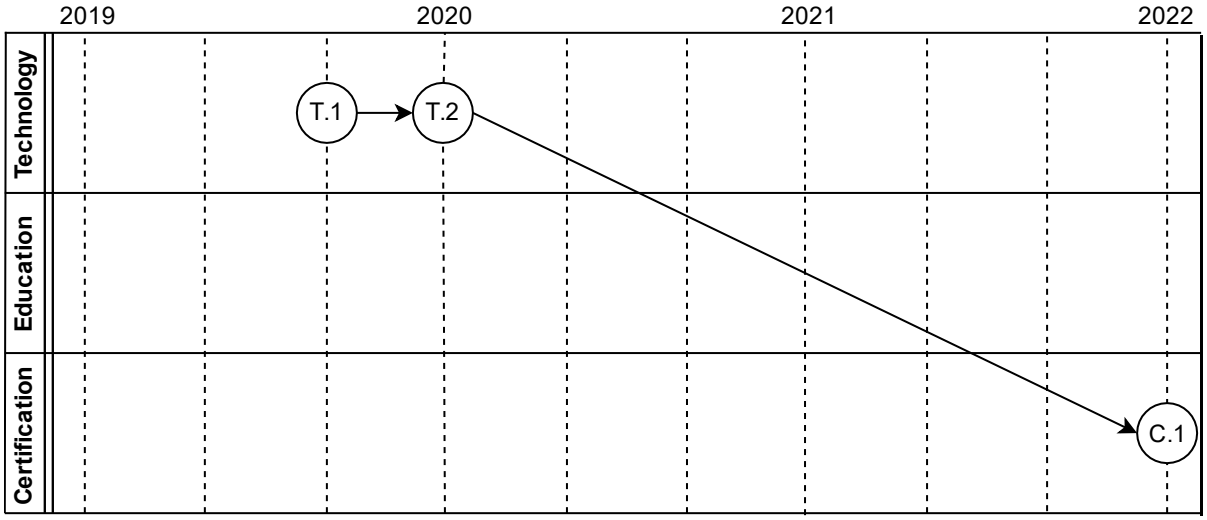

Figure 9: Timeline for expected completion of subgoals for Certification Organization and Support

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 on 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, like for instance, the notion of user control, of user empowerment, of user information. Tools are also needed in several domains of privacy. For instance, the GDPR provides very 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 behaviors, 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 freedom of physical persons, the measures taken will have to be strengthened. The rights of a data subject are also strengthened with better information and control over her data, following the user empowerment philosophy.

- **International:** The application of the European GDPR and its significant sanctioning power have 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 opposite, the GDPR comes into conflicts 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 American 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 localization, in the USA or elsewhere. Cultural differences with the European countries also account for major 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, being subject to a cat-and-mouse game with companies responsible for these privacy leaks.
  For instance we can mention 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?
  For instance, we can mention 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.
  For instance, we can mention 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.
  For instance, we can mention 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.
- The end-user is often inclined to declare herself 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 behaviors 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.
- Favor 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 application and high awareness of threats against privacy are excellent signs. - **Threats**: Privacy can go against other priorities. 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

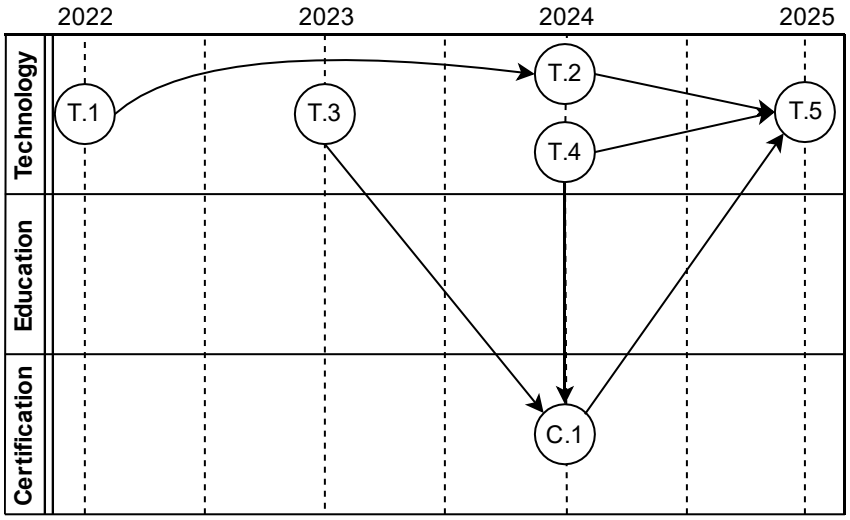

Figure 10: Timeline for expected completion of subgoals for User-Centric Data Governance

<table>
<tr><th>Stage/Dimension
Tx for Technology
Ex for Education
Cx for certification</th><th>Sector (JRC)</th><th>Domain (JRC)</th><th>Regulation</th></tr>
<tr><td rowspan="2">T1</td><td>Transversal to all sectors</td><td>Equivalent to Table 21</td><td></td></tr>
<tr><td colspan="3">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).</td></tr>
<tr><td rowspan="2">T2</td><td>Smart ecosystems, Transportation, Health, Digital infrastructure</td><td>Equivalent to Table 21</td><td></td></tr>
<tr><td colspan="3">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.</td></tr>
<tr><td rowspan="2">T3</td><td>Smart ecosystems, Transportation, Health, Digital infrastructure</td><td>Equivalent to Table 21</td><td></td></tr>
<tr><td colspan="3">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.</td></tr>
<tr><td>T4</td><td>Equivalent to Table 21</td><td>Assurance, Audit, and Certification; Data Security and Privacy;</td><td></td></tr>
</table>

		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 a little-studied topic. Nevertheless, a French “grand défi” has recently be launch around this question: “How to automate cybersecurity to make our systems resilient in the long term?”. An example of work comes from the Inria CTRL-A team that studies control techniques for the automated reaction to attacks. The team uses detection information to identify the appropriate defense 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 behavior in order to anticipate attacks, automate defense systems or even conduct correlation work relating to the attribution of attacks, but these issues remain unresolved 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 operative. This is a subject on which Europe could take the research and then industrial lead.

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, as we all know, and Europe is facing powerful countries (USA, China, Russia). In this context, a "cyberwar" cannot be ruled out. Even

without going that far, the protection of our European industrial assets is also necessary. The role of human operators remains of course major for cyber defense, but it is conceivable that in the near future there will be so many (maybe automated) attacks (i.e., a cyber-hurricane) that the automation of at least part of the response will be just essential to survive.
SWOT Analysis: - **Strengths:** 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:** This is a highly risked research topic. Success is by no means guaranteed. - **Opportunities:** Autonomous security is not currently operative. 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 defense.
Domain (JRC Taxonomy): Operational Incident Handling and Digital Forensics
Sector (JRC Taxonomy): Potentially all, with special importance in Energy, Transportation, Digital Infrastructure, Finance, Supply Chain
Relation to Emerging Technologies: We cannot totally exclude, even if for the time being the feasibility remains an issue, that 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

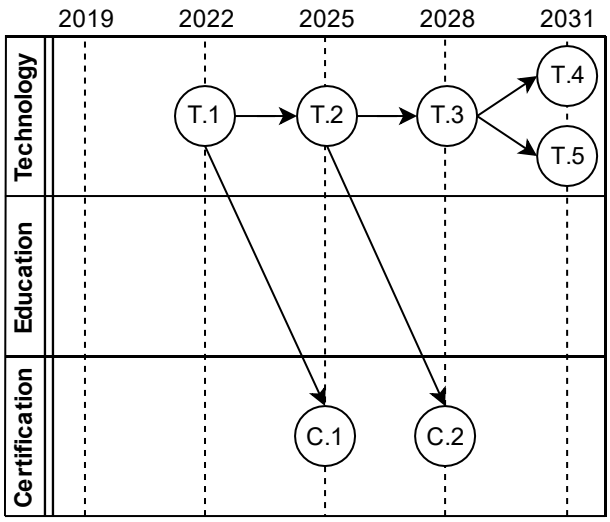

Figure 11: Timeline for expected completion of subgoals for Autonomous Security for Self-Protected Systems

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, is not rare. In this context, a proper definition of the policy would ask for a formal definition and verification of the set of rules. Also, 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. Nowadays, intrusion detection is essentially realized at the network level. If, as expected in the near future, the traffic was 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	Operational Incident Handling and Digital Forensics	

	Infrastructure, Finance, Supply Chain		
	Description (incl. obstacles): Accurately diagnosing 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 will very likely remain needed, as it is currently: alert correlation. 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. Considering that the security policy has been violated although preventive mechanisms have been used to enforce this policy, 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, of		

<table>
<tr><td></td><td colspan="3">course, 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).</td></tr>
<tr><td rowspan="2">C1</td><td>Potentially all, with special importance in Energy, Transportation, Digital Infrastructure, Finance, Supply Chain</td><td>Operational Incident Handling and Digital Forensics</td><td></td></tr>
<tr><td colspan="3">Description (incl. obstacles):

Detecting intrusions and anomalies: toward 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 (very) large majority of the activities analyzed are legal, even a (very) low rate of false positives can lead to many 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. Of course, this should be done without significantly penalizing the rate of false negatives: a balance must, therefore, be found, which depends on the detection approach, the system under surveillance and the nature of the activities analyzed.</td></tr>
<tr><td rowspan="2">C2</td><td>Potentially all, with special importance in Energy, Transportation, Digital Infrastructure, Finance, Supply Chain</td><td>Operational Incident Handling and Digital Forensics</td><td></td></tr>
<tr><td colspan="3">Description (incl. obstacles):

Ensure that the defensive response to attacks is relevant

Responding to an attack includes adapting 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.</td></tr>
</table>

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. Security here 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 we have 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.). Important American effort in 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. We propose to explore both directions. We will integrate security in a model-driven software engineering process, thereby giving substance to the security-by-design concept. We will, in particular, develop formal methods with high guarantees of security properties. In terms of validation, we shall develop 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): Defense, 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

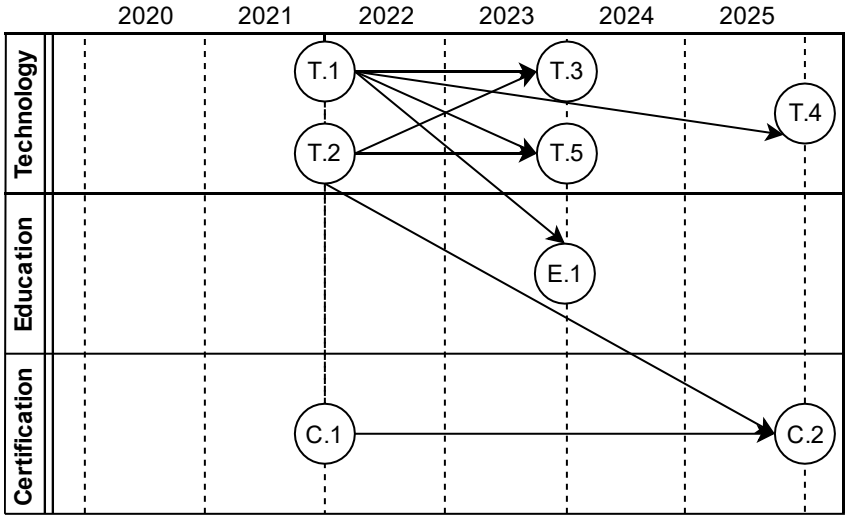

Figure 12: Timeline for expected completion of subgoals for Trustworthy Software

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 analyzing 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	Defense, Energy, Financial, Health, Nuclear, Transportation, Space	Assurance, audit and certification, software and hardware security engineering	
	Description (incl. obstacles): Make evolve existing certification schemes to take into account recent advances in formal methods-based techniques. Take an example from the aeronautics certification scheme where formal proofs can sometimes replace unit testing, identify processes where formal methods and automatization can aid in the security certification.		
C2	Defense, 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

Chapter 9 Positioning of Roadmap Challenges with Regard to the JRC Taxonomy Dimensions

This chapter contains the projection of the Roadmap Challenges 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 Management and Governance									
Network and Distributed Systems			■						
Software and Hardware Security Engineering			■						■
Security Measurements	■								
Legal Aspects		■		■					
Theoretical Foundations		■	■	■					■
Trust Management, Assurance and Accountability			■						

Table 27: 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 28: 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					■	■	■		
Defense	■					■	■		■
Digital Infrastructure	■				■	■	■	■	
Energy		■	■	■		■	■	■	■
Financial		■		■		■	■	■	■
Government and Public Authorities	■	■	■	■	■	■	■		
Health		■	■	■		■	■		■
Maritime			■			■	■		
Nuclear						■	■		■
Public Safety	■		■			■	■		
Tourism			■			■	■		
Transportation		■	■			■	■	■	■
Smart Ecosystems		■	■			■	■		
Space						■	■		■
Supply Chain			■			■	■	■	

Table 29: JRC Sectors covered by SPARTA roadmap challenges

Chapter 10 Conclusion

In this deliverable, we have described the context and process of obtaining the initial SPARTA roadmap. One basis for the roadmap is 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 is the overview of the existing national and international roadmaps, as well as the European JRC taxonomy. Based on all these information, we created seven long-term challenges (Program Challenges and Emerging Challenges) and described them using the roadmap template developed for this purpose. These challenges are the result of collaboration with SPARTA Program Leaders and Activity Leaders. Based on these long-term challenges we created a roadmap for cybersecurity research and innovation in Europe.

The long-term challenges are described in an extensive manner, encompassing multiple aspects. We begin by describing the problem, the final goal that should be strived for and the current state at European and international level. Furthermore, we looked at not only the research aspects but also at the industrial demand, social aspects and concrete benefits for the EU by tackling this challenge. We conducted a brief SWOT analysis in order to better characterize the challenge. Moreover, we related each challenge to the JRC taxonomy and the emerging technologies that we identified. For each challenge, we also created a preliminary timeline, 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. To ease the understanding of those challenge descriptions, we created a graphical representation summarizing the timelines for achieving the final goals through multiple stages.

This roadmap is the result of the first six months of SPARTA and is only an initial form of the roadmap that will be achieved. While it already encapsulates the vision of SPARTA partners about important challenges in the coming years, the SPARTA initial roadmap is meant to be dynamically adjusted during the project through six-month cycles. While the initial roadmap is heavily focused on technological topics, in the next version, we are planning to include more education and certification challenges. Furthermore, we plan to investigate long term challenges previously identified at the European level. Lastly, we are planning to continue with intensive collaboration with the existing SPARTA Programs in the identification and description of new challenges coming from the activities and research results of the partners in these Programs.

Chapter 11 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 12 Bibliography

[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