



D4.7 EU Cybersecurity & Privacy Final Roadmap

Author(s)	Mark Miller & Victoria Menezes Miller, CONCEPTIVITY
Status	Final
Version	V1.0
Date	31/07/2021

Dissemination Level

<input checked="" type="checkbox"/>	PU: Public
<input type="checkbox"/>	PP: Restricted to other programme participants (including the Commission)
<input type="checkbox"/>	RE: Restricted to a group specified by the consortium (including the Commission)
<input type="checkbox"/>	CO: Confidential, only for members of the consortium (including the Commission)



The work described in this document has been conducted within the project cyberwatching.eu. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 740129. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of its content.

Document identifier: Cyberwatching.eu – WP – D4.7	
Deliverable lead	CPT
Related work package	WP4
Author(s)	Mark Miller, Victoria Menezes Miller
Contributor(s)	Trust-IT, ICTL, UOXF, AON, DSME, AEI
Due date	31/07/2021
Actual submission date	31/07/2021
Reviewed by	Nicholas Ferguson, Trust-IT Paolo Modica, AON
Approved by	
Start date of Project	01/05/2017
Duration	51 months

Revision history

Version	Date	Authors	Notes
0.1	13.08.2020	M. Miller (CPT)	Table of contents
0.2	07.03.2021	M. Miller/V. Menezes Miller (CPT)	Revision of structure
0.3	19.03.2021	M. Miller/V. Menezes Miller (CPT)	Draft distributed for feedback
0.4	25.03.2021	M. Miller/ V. Menezes Miller (CPT)	Request for contributions
0.5	07.06.2021	P. Balboni/ L. Senatore/ A. Botsi (ICTL)	Sections 3.4 and 4.1.
0.6	14.06.2021	J. Bieliauskaite / J. Philpot (DSME)	Sections 2.3, 3.4 and 3.8
0.7	15.06.2021	M. Ramirez (AEI)	Sections 2.3.1, 2.4.1, 3.2, 4.4.1 and 4.4.2
0.8	22.06.2021	P. Modica (AON)	Sections 3.3
0.9	29.06.2021	M. Miller / V. Menezes Miller (CPT)	Sections 1, 2
0.10	07.07.2021	M. Miller/V. Menezes Miller (CPT)	Sections
0.11	08.07.2021	M. Miller/V. Menezes Miller (CPT)	Restructuring following contributions
0.12	09.07.2021	M. Miller/V. Menezes Miller (CPT)	Sections 2, 3
0.13	12.07.2021	M. Miller/V. Menezes Miller (CPT)	Sections 2, 3, 4
0.14	13.07.2021	D. Wallom (UOXF)	Section 3.7
0.15	14.07.2021	M. Miller/V. Menezes Miller (CPT)	Sections 3.1
0.16	14.07.2021	M. Miller / V. Menezes Miller (CPT)	Drafting in sections 1, 2, 3, and 4 / full document editing
0.17	14.07.2021	M. Miller / V. Menezes Miller (CPT)	Sections 3, 4, 5, 6

0.18	16.07.2021	M. Miller / V. Menezes Miller (CPT)	Sections 3.4, 5
0.19	19.07.2021	M. Miller / V. Menezes Miller (CPT)	Sections 2, 3, 4
0.20	19.07.2021	J. Bieliauskaite / J. Philpot (DSME)	Sections 2.3 and 5
0.21	20.07.2021	M. Miller / V. Menezes Miller (CPT)	Sections 3.4.3, 3.4.4
0.22	21.07.2021	N. Ferguson (Trust-IT)	Sections 2.3, 3.1, 3.2
0.22	23.07.2021	M. Miller / V. Menezes Miller (CPT)	Sections 2.5, 2.6, 5, Full document editing
0.23	23.07.2021	M. Miller / V. Menezes Miller (CPT)	Section 2.4, 2.5 – Additional contribution from D2.8
0.24	23.07.2021	M. Miller / V. Menezes Miller (CPT)	Sections 2.6, 5
0.25	26.07.2021	P. Balboni/ L. Senatore/ A. Botsi (ICTL)	Sections 2.1.2, 2.1.6.1
0.26	26.07.2021	J. Philpot (DSME)	Section 5.2.3
0.27	28.07.2021	M. Ramirez (AEI)	Sections 2.4, 2.4.1, 2.4.2, 2.5, 3.7, 5.2.1, 5.2.4, 5.2.8
0.28	28.07.2021	M. Miller / V. Menezes Miller (CPT)	Full edit
0.29	29.07.2021	N. Ferguson (Trust-IT)	Internal review
0.30	29.07.2021	M. Miller / V. Menezes Miller (CPT)	Implementing changes following review.
0.31	30.07.2021	M. Miller / V. Menezes Miller (CPT)	Sections 3.4, 3.4.1, 3.4.2, 3.4.4
0.32	30.07.2021	N. Ferguson (Trust-IT)	Executive Summary, Section 1
0.33	31.07.2021	M. Miller / V. Menezes Miller (CPT)	Sections 3.4.1, 3.4.2, Section 5
1.0	31.07.2021	N. Ferguson (Trust-IT)	Final version & PMB review

Executive Summary

Rather than recreating a new roadmap from scratch, this deliverable first and foremost represents a view of the existing roadmaps including conclusions and recommendations, so that we build upon the significant number of already existing roadmap efforts and modules, domains, categories, taxonomies and concepts. This is an important effort to understand the commonalities and the differences in approach. Furthermore, even non-European Union models and roadmaps have been considered.

Second, this deliverable also presents, summarises and shares the key points of the significant deliverables with the cyberwatching.eu project, especially those that are relevant for the roadmap. As such, this deliverable is thus the culmination of the project work for cyberwatching.eu and can be used as a building block for further efforts after the project is complete.

Table of Contents

1	Introduction	10
1.1	Structure of this document	10
1.2	Cyberwatching.eu Project in Brief	10
1.2.1	Understanding the R&I landscape	11
1.2.2	Contributing to a changing policy landscape	11
1.2.3	Supporting SMEs in understanding regulations and improving their cybersecurity posture	12
1.2.4	The new European Cybersecurity SME Hub	13
2	Review of Findings from Cyberwatching.eu Project	14
2.1	Key areas in the CS&P Roadmap	14
2.1.1	Data protection and privacy	14
2.1.2	Security by design and Privacy by design and by default	17
2.1.3	Training / Education / Awareness	17
2.1.4	Standards and Certification	18
2.1.5	Building trust - Establishment of an EU certification scheme	18
2.1.6	Emerging Technologies	19
2.1.7	International Dialogue	25
2.2	Risk Management	26
2.2.1	SMEs and information risk management	26
2.2.2	Cyberwatching.eu Cybersecurity Label	30
2.2.3	Cyberwatching.eu Cyber Risk Temperature Tool	31
2.3	Cyberwatching.eu Webinar of July 13, 2021	31
2.3.1	Horizon Europe and Digital Europe	32
2.3.2	Clustering of projects	32
2.3.3	Roadmapping activities	32
2.3.4	Standards and certification	34
2.3.5	Support to European SMEs	35
2.4	Cybersecurity and Privacy R&D ecosystem	35
2.4.1	Market Readiness Assessment	35
2.4.2	Identification of low developed spaces	36
2.5	Recommendations to EU on Projects	38
2.5.1	Recommendations from Cyberwatching.eu	38
2.5.2	Recommendations gathered from other EU projects	39
2.6	Summary of recommendations from Cyberwatching.eu Project	40
3	Roadmaps from European and international sources	50
3.1	EU Cybersecurity Strategy	50
3.1.1	Resilience, technological sovereignty and leadership	50
3.1.2	Operational capacity to prevent, deter and respond	51
3.1.3	Cooperation to advance a global and open cyberspace	51
3.1.4	European Data Strategy	51
3.2	European Agency for Network and Information Security (ENISA)	51
3.2.1	ENISA 2020 Strategy	51
3.2.2	Cybersecurity Research Directions for the EU's Digital Strategic Autonomy	53
3.3	European Cyber Security Organisation (ECSO)	54
3.3.1	Input to the Horizon Europe Programme 2021-2027	55
3.3.2	Input to the Digital Europe Programme 2021-2027	60
3.4	Four Pilots: CONCORDIA, CYBERSEC4EUROPE, ECHO, SPARTA	62
3.4.1	CONCORDIA	63
3.4.2	Cybersec4Europe	75

3.4.3	ECHO	100
3.4.4	SPARTA	102
3.5	SPARTA Roadmaps Analysis	124
3.5.1	SPARTA Analysis of European Cybersecurity National Strategies ...	124
3.5.2	National Roadmaps mapped to JRC Research Domains	125
3.5.3	National Roadmaps mapped to JRC Applications & Technologies ...	126
3.5.4	National Roadmaps mapped to JRC Sectors	127
3.5.5	European Cybersecurity Project Roadmaps	128
3.5.6	EU Project Roadmaps Mapped to JRC Research Domains	128
3.5.7	EU Project Roadmaps Mapped to JRC Appl. & Technologies	129
3.5.8	EU Project Roadmaps Mapped to JRC's Sectors	130
3.6	Joint Research Centre (JRC)	130
3.6.1	JRC Taxonomy	130
3.6.2	European Cybersecurity Atlas	133
3.6.3	The JRC Report "Cybersecurity – Our Digital Anchor – A European perspective	133
3.7	Relevant Academic/Research Results	133
3.8	National Institute of Standards and Technology (NIST) - USA	134
3.8.1	Priority area 1: Privacy risk assessment	135
3.8.2	Priority area 2: Mechanisms to provide confidence	136
3.8.3	Priority area 3: Emerging technologies	136
3.8.4	Priority area 4: De-identification risks and re-identification risks	136
3.8.5	Priority area 5: Inventory and mapping	137
3.8.6	Priority area 6: Technical standards	137
3.8.7	Priority area 7: Privacy workforce	138
3.8.8	Priority area 8: International and regulatory aspects, impacts and alignment	138
4	Evolving Landscape	139
4.1	European Regulatory Evolution Update	139
4.1.1	General Data Protection Regulation (GDPR) and NIS Directive	139
4.1.2	NIS2 Directive	139
4.1.3	ePrivacy Regulation	139
4.1.4	AI Regulation	139
4.2	Decision on the Cybersecurity Competence Centre in Bucharest	140
4.3	Evolution of ECSO (2.0 and 3.0)	143
4.4	Horizon Europe Programme and Digital Europe Programme	143
4.4.1	Horizon Europe Programme	143
4.4.2	Digital Europe Programme	144
5	Conclusions and Recommendations	146
5.1	Common denominators	146
5.2	Cyberwatching.eu Project	147
5.2.1	Project Radar	147
5.2.2	Light Cybersecurity Assessment and Label	148
5.2.3	The GDPR Temperature Tool and Information Notice Tool	149
5.2.4	Risk Assessment Tool	150
5.2.5	The ECSO SME Hub - Built upon the cyberwatching.eu marketplace core "engine"	150
5.2.6	SMEs – Overall Recommendations for The Future	151
5.2.7	Regulatory Landscape	151
5.2.8	R&D Landscape	152
5.3	Four Pilots & ECSO Cybersecurity Research Focus Areas Priorities	152
Annex A.	GLOSSARY	154

LIST OF FIGURES

Figure 2-1: Snapshot of changing landscape during life time of Cyberwatching.eu (webinar slide 13.07.21).....	14
Figure 2-2: Number of projects and its maturity for each priority identified by ECSO35	
Figure 2-3: Priorities ordered by the average maturity.....	36
Figure 2-4: Market maturity of cybersecurity solutions from R&D projects by vertical sectors.....	36
Figure 3-1: EU Cybersecurity Strategy.....	50
Figure 3-2: CONCORDIA'S Security Layers	64
Figure 3-3: CONCORDIA's Overview from technical perspective of most important directions in short-, mid-, and long-term timeframe	68
Figure 3-4: CONCORDIA Roadmap for Research and Innovation	68
Figure 3-5: CONCORDIA - Relationship between identified challenges & proposed recommendations	69
Figure 3-6: CONCORDIA Roadmap for Education and Skills.....	69
Figure 3-7: CONCORDIA's Roadmap on Economics.....	70
Figure 3-8: CONCORDIA's Roadmap on Investment Strategies	70
Figure 3-9: CONCORDIA's visualized Roadmap on Legal and Policy.....	71
Figure 3-10: CONCORDIA - Standardization & Certification Roadmap.....	74
Figure 3-11: CONCORDIA - Overview of different stakeholders and influencers of digital ecosystems	74
Figure 3-12: CyberSec4Europe's - Open Banking SWOT Analysis Summary.....	76
Figure 3-13: CyberSec4Europe - Supply Chain - SWOT Analysis Summary	79
Figure 3-14: CyberSec4Europe - Privacy-Preserving Identity Management SWOT Analysis Summary	82
Figure 3-15: CyberSec4Europe – Incident Reporting SWOT Analysis Summary	85
Figure 3-16: CyberSec4Europe – Maritime Transport SWOT Analysis Summary	89
Figure 3-17: CyberSec4Europe – Medical Data Exchange SWOT Analysis Summary	93
Figure 3-18: CyberSec4Europe – Smart Cities SWOT Analysis Summary.....	96
Figure 3-19: SPARTA Roadmap with the final goals to solve identified challenges	104
Figure 3-20: SPARTA Timeline of stages for technology, education and certification	105
Figure 3-21: SPARTA Timeline for expected completion of Comprehensive Cybersecurity Threat Intelligence (from T-SHARK).....	107
Figure 3-22: SPARTA Timeline for the expected completion of sub-goals for Security and Safety Co-Assessment (from CAPE).....	108
Figure 3-23: SPARTA D3.2 - Expected completion sub-goals for Complex Dynamic Systems of Systems (from CAPE)	110
Figure 3-24: SPARTA D3.2 - Expected completion sub-goals for High-Assurance Intelligent Infrastructures (from HAI-T)	111
Figure 3-25: SPARTA D3.2 - Expected completion sub-goals for Secure and Fair AI Systems for Citizen (from SAFAIR).....	113
Figure 3-26: SPARTA D3.2 - Expected completion sub-goals for Education and Training in Cybersecurity	115
Figure 3-27: SPARTA D3.2- Expected completion sub-goals for Certification Organization and Support.....	116
Figure 3-28: SPARTA D3.2 - Expected completion sub-goals for User-Centric Data Governance	118
Figure 3-29: SPARTA D3.2 - Expected completion sub-goals for Autonomous Security for Self-Protected Systems	119

Figure 3-30: SPARTA D3.2 - Expected completion sub-goals for Trustworthy Software	120
Figure 3-31: SPARTA D3.2 - Expected completion sub-goals for Quantum Information Technology	121
Figure 3-32: SPARTA D3.2 - Expected completion sub-goals of 5G Security	123
Figure 3-33 Cyberwatching Project Radar, Spring 2021	134
Figure 5-1: Key Priorities Importance Graph	146
Figure 5-2: EU Project Radar and Services	148
Figure 5-3: Cyberwatching.eu Cybersecurity Label for SMEs	149
Figure 5-4: GDPR Temperature Tool	150
Figure 5-5: Risk Assessment Tool for SMEs	150
Figure 5-6: Cyberwatching.eu Marketplace > ECSO	151
Figure 5-7: 4 Pilots & ECSO Perspective of Focus Area Priorities for Cybersecurity Research	152

LIST OF TABLES

Table 2-1: Research area priorities identified by SPARTA	33
Table 2-2: Cyberwatching Recommendations - EU Projects	39
Table 2-3: Cyberwatching Recommendations - Legal Aspects	43
Table 2-4: Cyberwatching Recommendations – Standards and Certification	44
Table 2-5: Cyberwatching Recommendations - Emerging Technologies, IoT	47
Table 2-6: Cyberwatching Recommendations - AI	49
Table 3-1: ENISA 2020 Strategy – Strategic Objectives and Target Achievements ..	52
Table 3-2: EU Cybersecurity research directions	54
Table 3-3: ECSO Input to the Horizon Europe Programme 2021-2027	56
Table 3-4: ECSO's Input to the Digital Europe Programme 2021-2027	61
Table 3-5: CONCORDIA Cybersecurity Threat Map	67
Table 3-6: CONCORDIA's Technology stack-related Recommendations	68
Table 3-7: Summary CONCORDIA Roadmap for Education and Skills	70
Table 3-8: CONCORDIA - Short-term standardization aims in standards & certification	71
Table 3-9: CONCORDIA - Mid-term standardization aims in standards & certification	72
Table 3-10: CONCORDIA - Long-term standardization aims in standards & certification	72
Table 3-11: CONCORDIA -Short-term certification aims in standards & certification	73
Table 3-12: CONCORDIA -Mid-term certification aims in standards &certification ...	73
Table 3-13: CONCORDIA - Long-term certification aims in standards & certification	73
Table 3-14: CyberSec4Europe – Challenges and Tools in Open Banking ²¹	78
Table 3-15: CyberSec4Europe - Open Banking Timeframe	79
Table 3-16: CyberSec4Europe - Challenges and Tools in Supply Chain	80
Table 3-17: CyberSec4Europe - Supply Chain Vertical Timeframe	81
Table 3-18: CyberSec4Europe - Challenges and Tools in Privacy-Preserving Identity Management ²⁴	83
Table 3-19: CyberSec4Europe Privacy-Preserving Identity Management Timeframe	84
Table 3-20: CyberSec4Europe - Challenges and Tools in Incident Reporting	86
Table 3-21: CyberSec4Europe Incident Reporting Timeframe	88
Table 3-22: CyberSec4Europe - Challenges and Tools in the Maritime Transport Vertical	90
Table 3-23: CyberSec4Europe- Maritime Transport Timeframe	92

Table 3-24: CyberSec4Europe: Challenges and Tools in the Medical Data Exchange Vertical	93
Table 3-25: CyberSec4Europe- Medical Data Exchange Timeframe	95
Table 3-26: CyberSec4Europe Challenges and Tools in Smart Cities.....	97
Table 3-27: SPARTA SWOT Analysis for Comprehensive Cybersecurity Threat Intelligence	106
Table 3-28: SPARTA – Sub-goals in Comprehensive Cybersecurity Threat Intelligence	107
Table 3-29: SPARTA SWOT Analysis for Security and Safety Co-Assessment	108
Table 3-30: SPARTA – Sub-goals in Security and Safety Co-Assessment	109
Table 3-31: SPARTA D3.2 – Sub-goals in Complex Dynamic Systems of Systems (from CAPE)	110
Table 3-32: SPARTA D3.2- Sub-goals in High-Assurance Intelligent Infrastructures (from HAIL-T).....	111
Table 3-33: SPARTA D3.2 - Sub-goals for Secure and Fair AI Systems for Citizen (from SAFAIR).....	114
Table 3-34: SPARTA D3.2 – Sub-goals for Education and Training in Cybersecurity	115
Table 3-35: SPARTA D3.2 – Sub-goals for Certification Organization and Support.....	116
Table 3-36: SPARTA D3.2 - Sub-goals for User-Centric Data Governance	118
Table 3-37: SPARTA - Sub-goals for Autonomous Security for Self-Protected Systems	119
Table 3-38: SPARTA D3.2 – Sub-goals for Trustworthy Software.....	120
Table 3-39: SPARTA D3.2 - Timeline for expected completion of sub-goals for Quantum Information Technology	122
Table 3-40: SPARTA D3.2 - Sub-goals of 5G Security.....	123
Table 3-41: SPARTA - Analysis of national cybersecurity roadmaps according to JRC’s research domains	125
Table 3-42: SPARTA - Mapping of National Cybersecurity Roadmaps to JRC Applications & Technologies	126
Table 3-43: SPARTA - Mapping of national cybersecurity roadmaps according to JRC Sectors	127
Table 3-44: SPARTA - Mapping of European Cybersecurity Roadmaps to JRC Research Domains	128
Table 3-45: SPARTA - Mapping European Cybersecurity Roadmaps to JRC’s Applications and Technologies	129
Table 3-46: SPARTA - Mapping of European Cybersecurity Roadmaps to JRC Sectors	130
Table 3-47: JRC Taxonomy	132

1 Introduction

This deliverable is an important effort to understand the commonalities and the differences in approach in the different cybersecurity Roadmaps. Furthermore, even non-European Union models and roadmaps have been considered.

During the length of this project, cyberwatching.eu has held several webinars, Concertation events, has launched several surveys, attended and presented at conferences and has regularly engaged with the four Competence Centre pilot projects. This deliverable, therefore, encompasses the findings of cyberwatching.eu through its wide stakeholder community engagement activities. In particular, the involvement of cyberwatching.eu with H2020 projects has been particularly productive as well as its engagement with the large SME community. The stakeholder community has also been covered in D4.4 “EU Cybersecurity & Privacy Interim Roadmap¹”, Chapter 2.

In addition, this deliverable presents a view of existing roadmaps including conclusions and recommendations, so that we build upon the significant number of already existing roadmap efforts and modules, domains, categories, taxonomies and concepts, such as JRC, the pilot projects (CONCORDIA, CyberSec4Europe, ECHO and SPARTA), ECSO, JRC, research and other entities.

1.1 Structure of this document

The deliverable takes the following structure:

- Chapter 2: Summarises and shares key points from significant deliverables of the Cyberwatching.eu project and which are relevant for the roadmap
- Chapter 3: Presents the results of other European Roadmaps and International Roadmaps
- Chapter 4: The current status evolving landscape is described, including the European Cybersecurity Competence Centre (ECCC)
- Chapter 5: Summary and conclusions

As such, this deliverable is thus the culmination of the project work for cyberwatching.eu and can be used as a building block for further efforts after the project is complete.

1.2 Cyberwatching.eu Project in Brief

We have come a long way since the cyberwatching.eu project began back in Spring 2017. The cybersecurity landscape in Europe was a very different and quite fragmented place: The NIS Directive had not long been adopted, ECSO and its WGs were holding their first meetings and the GDPR was still to come into force. Since then, the landscape has evolved and throughout this cyberwatching.eu and its partners have been monitoring, engaging, and contributing directly to the wide-range of measures the EU has adopted to shield the European Digital Single Market and protect infrastructure, governments, businesses and citizens.

With a number of sustainable assets, cyberwatching.eu leaves a lasting legacy which we believe can continue to contribute to this evolving landscape.

¹ Cyberwatching Deliverable D4.4: <https://www.cyberwatching.eu/d44-eu-cybersecurity-privacy-interim-roadmap>

1.2.1 Understanding the R&I landscape

Let's start first with the core of our work. With cybersecurity a key pillar of the EC's digital strategy cyberwatching.eu has delivered an EU Project Radar² which gives a clarity to a busy landscape. The radar provides an interactive "birds-eye" view of the complete collection of EU funded projects in the cybersecurity space. Over 260 projects are organized by high-level categories, their lifecycle stage and relative market and technology maturity. Users can also zoom in on technology and vertical sectors (defined by the EC's JRC cybersecurity taxonomy) in order to identify projects that are focusing on these areas. With 5 iterative versions dating back to 2018, the radar provides detailed analysis of the cybersecurity priorities over time. What is really special about the radar though is its live version. Managed directly by the projects it maps, researchers and innovators working in the EC R&I space can actually update their data in real-time and at the same time actually carry out a self-assessment on their market and technology readiness levels at the same time.

The radar offers a unique vision an ever-evolving landscape. It processes and analyses detailed landscape data for users such as policy makers, researchers and companies make swift yet statistically sound statements on the state of the art of the European cybersecurity and privacy research landscape.

Behind the radar lies detailed information managed by a community of R&I projects³ which have been funded by the EC. Realising the importance of supporting project-to-project collaboration to address technology and sector specific challenges, as well as joint dissemination actions to further market readiness, cyberwatching.eu has established six sector-specific clusters⁴ (health, energy, finance, critical infrastructure, GDPR, threat intelligence) involving over 25 projects and providing key support to deliver joint recommendations and over 10 webinars⁵.

Cyberwatching.eu partners are committed to sustaining these activities. We are in dialogue with the EC to understand how the radar, which represents single-entry point to the R&I landscape and community, can be fully exploited by the EC, and its entities such as the JRC and the new EU Competence Centre. Support to the clusters through the Horizon Results Booster and further joint webinars will continue so that the momentum built so far continues into the new era of funding that Horizon Europe (HE) and Digital Europe (DEP) Programmes provide.

1.2.2 Contributing to a changing policy landscape

The announcement of the new EU Competence Centre in Bucharest earlier this year represents a watershed moment for a truly European approach to cybersecurity. Contributing to this, Cyberwatching.eu has played a constructive role in facilitating collaboration between four Competence Centre Pilot projects since their conception in 2019. From organizing the first of a number of joint-public workshops to providing documentation detailing activities and respective roadmaps (included in this document), we have consistently engaged and contributed to supporting their dialogue and alignment between them.

The European Union and the EU Member States are building the necessary cybersecurity culture and capabilities to resist and counteract the very real and ever-

² Project Radar: <https://radar.cyberwatching.eu/radar>

³ R&I Projects: <https://www.cyberwatching.eu/projects>

⁴ Project Clusters: <https://www.cyberwatching.eu/cybersecurity-and-privacy-project-clusters>

⁵ Cyberwatching Webinars: <https://www.cyberwatching.eu/webinar>

changing cyber threats and cyber-attacks. In the duration of the cyberwatching.eu project, the regulatory landscape has evolved through a number of regulatory tools, including regulations, directives and manifold opinions, guidance, and tools aiming to guarantee a higher level of data protection to European citizens and an increased legal certainty. We captured this transformation in a key document “Building Strong Cybersecurity in the European Union”⁶ presented by the EC’s delegation visit to the US in 2019.

In 2018, the General Data Protection Regulation (GDPR) became the first landmark in the evolutionary landscape in Europe safeguarding data protection, transparency, purpose limitation, and many more rights and guarantees to data subjects. Following that, the Directive on security of network and information systems (NIS Directive) imposed a minimum standard on operators of essential services and digital services ensuring that the European critical infrastructure would be harmonized.

The cybersecurity and technology landscape moving fast more often than not, much faster than legal regulations can cater for. New technologies such as AI, Blockchain and IOT have emerged and with them new challenges which need to be addressed. Cyberwatching.eu has provided a robust package of recommendations⁷ facing both the policy makers and the Supervisory Authorities, to address stakeholders’ needs in this area. Clear explanations of the fundamental obligations included in the GDPR, are best provided by the experts that practice and apply the GDPR on a day-to-day basis, making the cyberwatching.eu partners the most appropriate resource of creating this impact. As we see next, the ultimate aim of merging legal and technical knowledge and practical observation of reality was to develop online tools that are meant to complement one another, resulting in self-assessment tools that provide handy self-explanatory legal and practical recommendations for all stakeholders, including SMEs.

1.2.3 Supporting SMEs in understanding regulations and improving their cybersecurity posture

SMEs have a vital role to play in the development of Europe’s cybersecurity capacities and digital sovereignty. SMEs make up the back-bone of the European economy accounting for 99% of businesses in Europe. A clear need for reliable and trusted self-assessment resources for SMEs to understand the GDPR and their cybersecurity posture was identified early in the project and addressed.

The GDPR Temperature Tool⁸ and Information Notices Tool⁹, provide expert guidance to SMEs providing an overview of their strengths and weaknesses in their compliance posture, and immediate recommendations on how to move forward, and suggestions of tools, software, and services they can consider to improve their compliance.

With the EU Cybersecurity Act is another milestone for Europe coming into force less than a year ago to provide an EU-wide harmonised framework to certify ICT products and services. cybersecurity certification can be a market differentiator for businesses. Certifications can help companies act with confidence and assure their customers and partners of their ability to defend themselves from cyberattacks and data breaches. However, for an SME, micro-enterprise or start-up, taking the first steps to certification

⁶ Building a strong EU Union <https://www.cyberwatching.eu/publications/building-strong-cybersecurity-european-union>

⁷ cyberwatching.eu recommendations: See D3.4, 3.5 and D3.7

⁸ GDPR Temperature Tool: gdprtool.cyberwatching.eu/Pages/Home.aspx

⁹ Information Notices Tool : <https://infonoticetool.cyberwatching.eu/Pages/Home.aspx>

can be both complex and daunting. By delivering the Cybersecurity Label¹⁰ in partnership with the the global leader of Testing, Inspections and Verifications SGS, cyberwatching.eu has provided a cost-effective resource for SMEs to understand and take first step towards certification. By including a lightweight approach of several and existing certification schemes, this self-assessment exercise includes the security requirements that any organization should comply with in order to demonstrate that it has securely implemented basic logical systems and measures to protect their assets against cyber-threats.

The online resources above as well as the Risk Management Temperature Tool¹¹ and various SME guides will live on through the Spanish Cybersecurity Digital Innovation Hub CyberDIH¹², which is part of a broader EU network.

1.2.4 The new European Cybersecurity SME Hub

The cyberwatching.eu marketplace¹³ is a unique platform which showcases both CS&P results from R&I projects in a market-oriented way and together with services and products from European SMEs. Through collaboration with ECSO to address their need for an SME Hub, a Marketplace v3 will be handed over and sustained by ECSO. The hub will become a lasting legacy of cyberwatching.eu.

A key driver for the marketplace and ECSO SME Hub is to increase the trust and confidence in European products and services, so that buyers can discern which products, services and solutions can be trusted. It is also a market support and networking tool for European Cyber SMEs, helping them to create more market transparency and to reach out far beyond their traditional home markets, which are usually nationally or regionally limited. Finally, the Hub shall give the possibility to serve as a market differentiator between SMEs based on their broadness of service, quality and capability to deliver.

So, although cyberwatching.eu comes to an end, we see a new beginning with partnerships formed between project partners, a legacy of lasting and sustained outputs and new challenges and horizons with the HE and DEP.

¹⁰ <https://gtt.cyberwatching.eu/Pages/Home.aspx>

¹¹ <https://cyberrisk.cyberwatching.eu/Pages/Home.aspx>

¹² <https://www.cyberdih.com/en/>

¹³ <https://cyberwatching.eu/market-products-list>

2 Review of Findings from Cyberwatching.eu Project

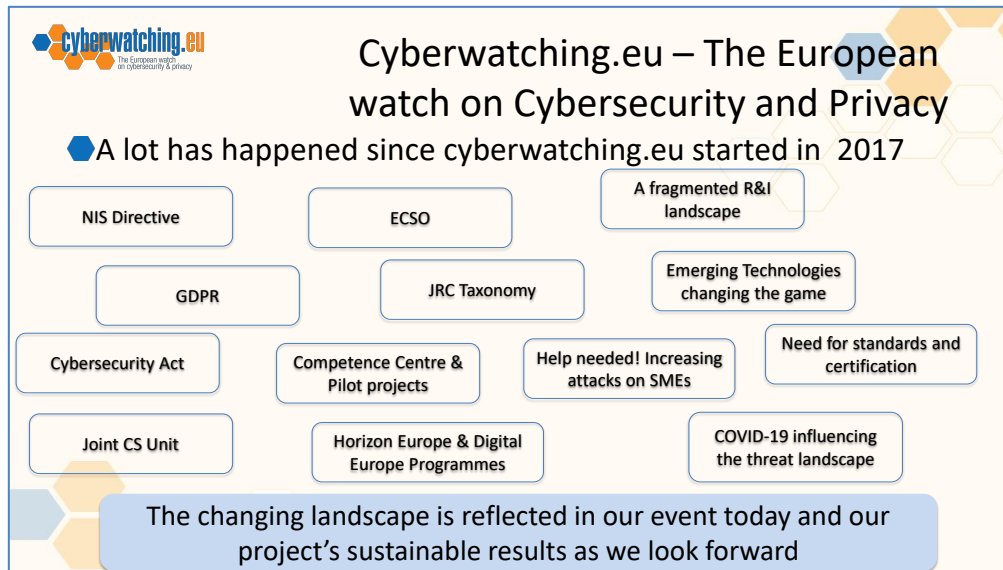


Figure 2-1: Snapshot of changing landscape during life time of Cyberwatching.eu (webinar slide 13.07.21)

In the life-time of the cyberwatching.eu project, many events have taken place influencing the cybersecurity landscape and roadmap. This section presents some of the challenges, recommendations and/or conclusions (taken from several deliverables during the length of the cyberwatching.eu project) and from which the building blocks of the roadmap evolved.

2.1 Key areas in the CS&P Roadmap

The following key areas emerged as priorities:

- Data protection and privacy
- Cybersecurity and privacy by design
- Training / Education / Awareness
- Standardization and privacy
- International Dialogue
- Building trust - Establishment of an EU certification scheme
- Emerging Technologies

2.1.1 Data protection and privacy

Data protection of citizens relies on a sound legal and policy framework. Deliverable D3.4 “EU Cyber Security Legal and Policy Aspects: Preliminary Recommendations and Road Ahead” presents recommendations to policy-makers with regards to the interaction between the General Data Protection Regulation (GDPR) and the Directive on security of network and information systems and the challenges brought about by the deployment of new technologies like Artificial Intelligence, Internet of Things and Blockchain. It also collected proposals from EU projects on areas of research and policy solutions within the scope the two main strategic elements which will shape the EU landscape in cybersecurity and privacy: Horizon Europe and Digital Europe Programme. Recommendations are presented below¹⁴:

¹⁴ D3.4 available on cyberwatching.eu website:

https://www.cyberwatching.eu/sites/default/files/D3.4%20EU%20Cybersecurity%20legal%20and%20policy%20aspects_preliminary%20recommendations%20and%20road%20ahead.pdf

Recommendations from Deliverable D3.4:

- **“European self-assessment tool”**: it is recommended that the EC invests in research initiatives in order to create a tool, or several ones, that can serve as more practical instruments to increase the compliance of all organisations (multinationals, medium, small and micro enterprises, research projects) under the scope of the GDPR.
- **Updated methodology to assess the severity of data breaches and feedback on tool for notification of data breaches**: need for further guidelines on the assessment of the severity of breaches and a methodology on how to manage and react to the breaches. This recommendation could be achieved by updating of the existing methodology from ENISA.
- **European tool for Data Protection Impact Assessment**: the creation of a tool for data protection impact assessments, which could compile the several applicable national black lists, is highly recommended.
- **Encouraging the creation of codes of conduct to demonstrate compliance**: It is recommended that in the context the DEP’s objectives the European Commission encourages the creation of codes of conduct, pursuant to art. 40 GDPR; these codes of conduct should take into account the specific features of the processing sectors as well as the specific needs of micro, small and medium-sized enterprises.
- **European certifications, seals and marks on data protection**: the European Commission shall encourage, in particular at the European level, the establishment of data protection certification mechanisms and data protection seals and marks described in articles 42 GDPR. For this purpose, there is a need for a strategic research initiative which will propose a structured approach to certify tools and other instruments created by private entities as compliant at European level.
- **Guidelines on methodology for risk assessment especially focused on each sector of the OES (NIS Directive) – which are essentially the critical infrastructure of countries**: ENISA could work together with the DEP stakeholders, with the aim of producing practical guidelines for assessing the risks in the essential services of member states at a centralised European level.
- **Clarifications on the intricacies between GDPR and NIS**:
 - DEP could use industry to shed light on the procedures that take place in real time of such circumstances, and the research component (Horizon Europe) should find the most time-efficient and compliant method of managing notifications that fulfill the requirements of both the NIS Directive and the GDPR
 - Policy-makers could provide guidance for organisations on the extent to which sanctions will be applied for both legislations and how such violations will be regarded by competent authorities and member states.
- **Practical clarifications on the application of the GDPR to blockchain** are very much needed for this technology and the law to coexist. It should be clarified how those systems could be specifically crafted, in careful consideration of the rules set by the principles of data protection by design and, specifically, of fairness by design, to ensure that individuals’ privacy and real control over their data is afforded to them:
 - While some principles remain largely unaffected by the technology, such as the principle of lawfulness and purpose limitation, and others may even find themselves enhanced by the additional functionalities brought about by blockchain, such as the principle of fairness, others still appear to frontally collide with its ‘set-in-stone’ nature, namely the principles of data minimisation and storage limitation which, in

turn, may affect the ability to effectively exercise some data subject rights regarding personal data stored 'on-chain' (such as the right to rectification or erasure).

- It is also not a simple matter to identify and agree on the data processing roles played by the participants in a blockchain-based system.
- An even more complicated matter is to ensure that the formal requirements tied into these roles are met, such as the need for a contract or other legal act containing a set of minimum obligations to be entered into with each processor engaged by a controller, in light of Art. 28 GDPR – this problem currently appears not to have a practically viable solution when considering public blockchains.
- The matter of international transfers and the implementation of the requirements for their lawfulness raises similar difficulties in light of the decentralised nature of blockchain-based systems.

In addressing the recommendation regarding “European self-assessment tool”, cyberwatching.eu delivered two online GDPR-related self-assessment tools in the form of the GDPR Temperature Tool¹⁵ and the Information Notices Tool¹⁶. These are described in section 5.2.4. In July 2021, cyberwatching.eu published its deliverable “D3.7 EU White Paper around legal compliance and policy statements including recommendations”. The White Paper highlights the progress made since D3.4¹⁴ and the remaining challenges for the cyberwatching.eu’s stakeholders on the topic of legal compliance. Seeing as cyberwatching.eu is the European watch on cybersecurity & privacy, many stakeholders are either developing or deploying emerging technologies, and this is the main reason why the scope of the legal challenges and legal recommendations provided tackle the two emerging technologies of Artificial Intelligence and Internet of Things. The main recommendations from the White Paper are listed below.

Recommendations from Deliverable D3.7

Recommendations on GDPR:

- a) *Creation of a single space to collect all the different types of guidance (opinions, guidelines, instruments, tools, self-assessments) created by Supervisory Authorities based on the GDPR 'topic' or GDPR 'obligation' to ensure easy access availability.*
- b) *Publication of a systematic Methodology for GDPR risk assessments which will be available for all stakeholders in every Member State.*
- c) *Allocation of specific priority areas that require instruments or guidance to different Supervisory Authorities, in order to ensure efficiency and consistency in the guidance provided to organisations.*
- d) *Updated methodology to assess the severity of data breaches and feedback on tool for notification of data breaches by modernizing of the existing methodology from ENISA.*
- e) *European tool for Data Protection Impact Assessment which could compile the several applicable national “black lists”.*
- f) *Publication of guidelines and recommendations on Data Transfer Impact Assessment.*
- g) *Creation of a data transfer impact assessment, which will assist organisations to assess all relevant factors and considerations before carrying out data transfers outside the EEA.*
- h) *Further research on managing notifications that fulfill the requirements of both the NIS Directive and the GDPR.*

¹⁵ <https://gdprtool.cyberwatching.eu/Pages/Home.aspx>

¹⁶ <https://inforoticetool.cyberwatching.eu/Pages/Home.aspx>

2.1.2 Security by design and Privacy by design and by default

Emerging technologies can require an innovative and unconventional approach to compliance, to facilitate organisations in their efforts to apply the risk-based approach to compliance, the below recommendations must be considered.

Recommendations from Deliverable D3.4:

Guidance on implementation of data protection by design and by default in emerging technologies: further research and guidance on how privacy by design and by default can be involved in industry standards for emerging technologies is highly recommended.

*Need for further guidelines on the application of principles of **data protection by design/default** and data minimisation for IoT deployments.*

2.1.3 Training / Education / Awareness

Throughout the project, the problem of training / education / raising awareness in the field of cybersecurity, and retaining European talent has been raised. The following recommendations are relevant:

Recommendations from Deliverable D3.3:

A THIRD RECOMMENDATION is EC funding for **Raising Awareness and Education in Cybersecurity Standards and Certification** for both the Public and Private sectors. This recommendation stems from the repeated request in our survey, and at events, to provide information, education and guidance so that both public and private sectors in order to move forward with the essential knowledge to address this gap of expertise in standards and certification. It is already recognised that Europe does not have enough of skilled experts which the industry needs and stakeholders lack the cybersecurity knowledge.

One of the most important problems in a company is the high level of employee turnover. Currently, with a dearth of cybersecurity experts in the European workforce, finding the right expert is challenging. Therefore, the company should remember that it is easier to explain the core business knowledge than technical skills. The technical knowledge that an employee has is one of the main and most important aspects to be assessed in cyber risk management. Better training for staff and education at both university level and before is a key aspect of this.

Recommendations from Deliverable D3.4:

Education and training to raise industry awareness: research initiatives should find the best method to educate the industry operating in the field of emerging technologies on ways to address the existing challenges and give practical instructions on how to concretely achieve compliance.

From the Concertation Event of 2018, Deliverable D3.2:

Top R&I Challenges:

<ol style="list-style-type: none"> 1) Certification 2) Education & Awareness 3) Social & Ethical (social pressure) 4) European Values (how to address these) 5) Global Cooperation
Top new collaboration opportunities and new ideas:
<ol style="list-style-type: none"> 1. Sharing CTI and risk models between projects 2. Need to better facilitate the collaboration between business and academia to synergise research e.g. development of Impact Models 3. Open labs & tools 4. Education and training/ raising awareness 5. Develop database of best practises

2.1.4 Standards and Certification

The subject of standards and certification has been described in Deliverable D3.3 “White Paper on cybersecurity standard gap analysis”, which also contains the results of a survey on the gaps in the field of standards and certification. While many cybersecurity standards and certification solutions already exist, it is the general consensus that the biggest gap occurs with respect to **fragmentation and the often national nature of the systems (without mutual recognition) raising issues such as challenges in interoperability, market fragmentation and increased cyber risk.**

Recommendation from cyberwatching.eu deliverable D3.3:
<ol style="list-style-type: none"> 1. The issues of Mutual Recognition and Harmonisation must be addressed due to the national nature of many standards and certification systems 2. Further efforts must be made in order to raise awareness concerning the available accepted standards and certification, as well as the certification process in case of multi-party composition of products and solutions. 3. EC funding should be targeted toward Raising Awareness and Education in Cybersecurity Standards and Certification for both the Public and Private sectors. 4. International Cooperation is an area for opportunities to benchmark best practices and standards that may already exist as a way to not “reinvent the wheel”, however, caution is urged in taking care not to immediately co-opt existing standards that may put European industry at a disadvantage. 5. The cost issue for SMEs looking toward standards and cybersecurity certification must be addressed. SMEs must be able to access standards and the related certification without breaking the bank. Self-assessment and other low-cost solutions must be explored. 6. The R&I community should look address the fast-evolving area of Internet of Things (IoT) with respect to cybersecurity standards and certification. 7. Elaborate a common research agenda across EU Member States (MS). Through the vehicle of the ERC, open specific calls for projects in the area of cybersecurity with clear aims and requirements in developing in areas of relevance to standards in cybersecurity

2.1.5 Building trust - Establishment of an EU certification scheme

The overall goal of cybersecurity standards and certification is to increase the trust and confidence in European products and services, so that buyers can discern which products, services and solutions can be trusted. This is also a direct effect in supporting

the competitiveness of European industry and clearly addressing the protection and security of the European citizen. The recommendations below have been extracted from Deliverable D3.3 “White Paper on cybersecurity standard gap analysis”.

Recommendation from cyberwatching.eu Deliverable D3.3:

A THIRD RECOMMENDATION is EC funding for **Raising Awareness and Education in Cybersecurity Standards and Certification** for both the Public and Private sectors. This recommendation stems from the repeated request in our survey, and at events, to provide information, education and guidance so that both public and private sectors in order to move forward with the essential knowledge to address this gap of expertise in standards and certification. It is already recognised that Europe does not have enough of skilled experts which the industry needs and stakeholders lack the cybersecurity knowledge.

“A FOURTH RECOMMENDATION - **International Cooperation** was identified as an area to be looked upon for opportunities to benchmark best practices and standards that may already exist as a way to not “reinvent the wheel”, however, caution is urged in taking care not to immediately co-opt existing standards that may put European industry at a disadvantage. From the results of ongoing projects in US and JP, several common areas of interest for collaboration emerged.”

A FIFTH RECOMMENDATION is to address the **cost issue for SMEs** looking toward using cybersecurity standards and certification. As SMEs are the innovation engine especially in the cybersecurity realm, it is important that they can access standards and the related certification – with cost being a huge issue for them, self-assessment and other low-cost solutions must be explored since relying on specialised experts is very costly, including the cost of specific standards. The current lengthy and complicated process only adds to costs and finally acts as a hindrance to innovation. Again, ECSO Working Group 1 has efforts to address this issue.

A SIXTH RECOMMENDATION is to address the Internet of Things (IoT) which was as well identified in our survey as an area where there is **evidence of a lack of cybersecurity standards and certification** and this does require some concerted effort on the part of the research and industrial community to address this fast-evolving gap. This is also a well-known area that will be on the agenda of organisations such as the IoT Forum and ECSO.

A SEVENTH RECOMMENDATION is to elaborate a common research agenda across EU Member States (MS). Through the vehicle of the ERC which is available to all MS scientists, it would be sensible to open out specific calls for projects in the area of cybersecurity with clear aims and requirements on developing in areas of relevance to standards in cybersecurity. This call should be preceded by a large publicity campaign. It would not be possible to get MS themselves to operate internal funding in a coherent manner so using academic research focused central money such as ERC would be a more cost-effective mechanism. There should also be the continued push for EC sponsored research to be fully open access not only in the final publication but also in the protocols, software and data used within the projects supported.

Recommendation from cyberwatching.eu deliverable D3.3:

“A FOURTH RECOMMENDATION - **International Cooperation** was identified as an area to be looked upon for opportunities to benchmark best practices and standards that may already exist as a way to not “reinvent the wheel”, however, caution is urged in taking care not to immediately co-opt existing standards that may put European industry at a disadvantage. From the results of ongoing projects in US and JP, several common areas of interest for collaboration emerged.”

2.1.6 Emerging Technologies

In the Covid-19 pandemic time, the importance and reliance on technology grew exponentially and caused an evolution of technology some of which was already in existence for some time, such as video conferencing. Furthermore, this led to a

proliferation and ubiquitous use of capabilities which had not been fully utilized previously, such as distance-learning, teleworking, personal communications, transactions (be it banking, health or other), video conferencing, use of wikis, communication interactions, virtual environments and other technologies which did not require physical presence.

Recommendations from Deliverable D3.4:

- **Practical guidelines on compliance of automated processing in the context of emerging technologies:** The DEP can prioritise to give guidance on how to demonstrate compliance where the automated processing activities may not be possible or easy to disclose in information notices.
- **Structured cooperation between policy makers, the research and the market/industry:** the DEP should aim at drafting a structured flow of information that facilitates the continuous sharing of feedback between policy makers, research initiative and industry on matters regarding emerging technologies.
- **Guidelines on anonymisation tools and pseudonymisation mechanisms:** it is recommended that the European Commission stimulates the creation of guidelines on anonymisation and pseudonymisation mechanisms, which are acceptable as being able to address the challenges of emerging technologies.

Recommendations from Deliverable D3.7

Recommendations on emerging technologies:

- a) *Creation of practical tools focusing on compliance of emerging technologies, that are kept up to date according to the industry standards and state of art as well as rate of change of the technologies.*
- b) *Education and training to raise industry awareness in the field of emerging technologies.*
- c) *Structured cooperation between policy makers, the research and the market/industry.*

2.1.6.1 Internet of Things (IoT)

The Internet of Things (IoT) allow for the connection of common objects (e.g., cell phones, wearable devices, cars, appliances) to the Internet with the purpose of exchanging information between each other.¹⁷ These IoT systems inevitably rely on the processing of personal data to such an extent that the concept of IoT has been often linked, by the Article 29 Data Protection Working Party,¹⁸ to the notions of 'pervasive' and 'ubiquitous' computing, which raise new and crucial personal data protection and privacy.¹⁹ Due to the new challenges emerging in this sector, the Consortium deemed it necessary to delve into this sector and provide policy makers, and supervisory authorities with suggestions and recommendations that could be the

¹⁷ European Data Protection Supervisor, *Internet of Things*, available at: https://edps.europa.eu/data-protection/our-work/subjects/internet-things_en.

¹⁸ The Article 29 Data Protection Working Party was an independent European working party that dealt with issues relating to the protection of privacy and Personal Data until 25 May 2018 (entry into application of the GDPR), at which point it was replaced by the European Data Protection Board.

¹⁹ Article 29 Data Protection Working Party, *Opinion 8/2014 on the on Recent Developments on the Internet of Things* (16 September 2014), p. 4, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

focus in the near future. Below we summarise the recommendations collected from the work carried out in the entire duration of the project.

Recommendations from Deliverable D3.4¹⁴:

- **Need for further guidelines on the application of principles of data protection by design/default and data minimisation for IoT deployments:** such guidelines should give advice on how to concretely inform users as per Art.s 12-13-14 GDPR, which legal basis is permitted to process personal data and how data subjects can effectively exercise their rights. Moreover, such guidelines should address end-to-end security during the entire data-lifecycle, given that the machines performing data processing are typically under the control of different organisations (acting as controllers or processors as the case may be) without an overarching orchestration and control over the data.
- **Practical guidelines on the allocation of privacy roles in IoT environments in the light of the GDPR** are needed, since IoT poses strong challenges to the allocation of privacy roles of the several parties involved in processing. The use of data protection contracts (i.e., Privacy Level Agreements) - other than data processing agreements pursuant to Art. 28 or joint-controllership agreements pursuant to Art. 26 GDPR – should be considered, whereby, regardless of the privacy rules, duties, obligations and responsibilities of the parties involved are clearly spelled out.

Recommendations from Deliverable D3.5:

IoT

IoT and Data Minimisation

- It is recommended that IoT developers/providers consider to **more comprehensively design IoT devices and services with the principle of data minimisation in mind**, incorporating the concepts of data protection by design and by default into the development process. In particular, as has been noted by the Article 29 Data Protection Working Party in the past, the principle of data minimisation “*specifically implies that when personal data is not necessary to provide a specific service run on the IoT, the data subject should at the least be offered the possibility to use the service anonymously*”.
- One of the ways in which this could be done, which would also address the problem of individuals’ lack of control over IoT data flows, would be for developers to consider **creating ‘privacy dashboards’ or ‘privacy interfaces’ for individuals** – these dashboards/interfaces, which could be available on specific devices (such as an individual’s mobile phone), could act as a control centre for that individual’s IoT devices and services, offering information and options concerning data receipt and transmission for each device or service.
- **It is recommended for Controllers to consider if this problem which could be addressed by policy and regulation, where stricter requirements on data collection and transmission could be enforced on IoT developers.** Possible solutions could include an obligation to build in ‘do not collect’ switches or permissions into IoT devices and services, so that individuals can disable or limit collection and transmission of data before even activating the device or service.

IoT and Purpose of limitation:

- The imposition of limitations or further requirements on subsequent processing of personal data, collected and shared between IoT-connected devices and services, seems to be a reasonable solution. **It is recommended to provide individuals with control over which data may be collected and transmitted, through the use of**

dashboards, privacy centres or other privacy enhancing technologies, - this would already be a large step to achieve this goal.

- **It is recommended that contractual limitations between stakeholders (through Data Management Agreements) be imposed on the further processing of received personal data** as this could be a key step in ensuring that appropriate limitations are in place, particularly in the absence of stricter and clearer policy on IoT data collection, sharing and repurposing.

IoT and Transparency and lawfulness:

- Two suggestions to help comply with the principle of transparency are the use of **just-in-time notifications and periodic notifications**, which may allow developers to deliver specific and relevant information to individuals at times when they are most likely to be able to apprehend such information. Furthermore, as noted above, **the development of privacy dashboards or control centres for individuals may be fundamental in this respect**, as it can allow not only the creation of a central point where information on the processing activities undertaken may be accessed, but also where individuals may set their preferences in regards to data collection/transmission and, potentially, also exercise their rights under the GDPR directly (e.g., accessing, rectifying, deleting or exporting personal data captured by IoT-connected devices).
- It is recommended that **further research continue and guidelines be produced on effective means by which information on processing activities carried out via IoT can be delivered to individuals** – particularly those who may be captured by the sensors of such devices, without necessarily owning them or having activated them (such as visitors or passers-by).

IoT Security:

- It is recommended that further research continue and the development **guidelines and procedures be developed to assist controllers in carrying out regular monitoring and testing activities, when faced with systems composed of multiple IoT-connected devices.**
- Furthermore, an additional consideration would be the **implementation of end-to-end encryption regarding all data collected and transmitted by and between IoT-connected devices and services.**
- It is recommended that further security measures and best practices which should be considered include those within **ENISA's guidelines on Good Practices for Security of Internet of Things.**

Recommendations from Deliverable D3.7 (July 2021)

Recommendations on Internet of Things:

- Need for further guidelines on the application of principles of data protection by design/default and data minimisation for IoT deployments.*
- Practical guidelines on the allocation of privacy roles in IoT environments in the light of the GDPR.*
- Guidance or further research into the key aspects to be regulated between stakeholders, via Data Management Agreements (in particular, where the controller-to-controller terms are concerned), to provide tools for stakeholders to effectively self-regulate.*
- Impose limitations or further requirements on subsequent processing of personal data, collected and shared between IoT-connected devices and services.*
- Guidelines on effective means by which information on processing activities carried out via IoT can be delivered to individuals – particular those who may be captured*

by the sensors of such devices, without necessarily owning them or having activated them (such as visitors or passers-by).

- f) *Guidelines and procedures to assist controllers in carrying out regular monitoring and testing activities, when faced with systems composed of multiple IoT-connected devices.*
- g) *Ensure that IoT developers and users are bound by ethical considerations in their activities, further research and the development of clear, understandable and practical guidelines developing the concept of Fairness by Design (including, for example, a checklist which could be relied on by IoT-based solution developers) would be welcomed.*

2.1.6.2 Artificial Intelligence

Artificial intelligence (AI) is a flexible and interchangeable emerging technology that has a wide-ranging implementation and integration in systems, software and devices of varying sector.²⁰ From the data protection perspective, AI is typically used as a tool for automated decision-making and profiling, by leveraging algorithms to process large volumes of data.²¹ In this context, the main challenges arise when the processing activities carried out by means of AI are capable of leading to automated decisions which produce legal, or similarly significant effects on data subjects.²² Below we summarise the recommendations collected from the work carried out in the entire duration of the project.

Recommendations from Deliverable D3.4:

- **Guidelines on AI/machine learning and data minimisation:** it is recommended that policy makers strive for research initiatives that look into how to concretely deploy AI and machine learning models, respect the principle of data minimization, storage limitation and data accuracy (Article 5 (1) (b), (c), (d) GDPR).
- **Solutions to address complexity of processing in the context of AI and principle of transparency:**
 - it is recommended to invest in researching initiatives which aim at focusing on how to safeguard and ensure transparency when the complexity of emerging technologies escalates constantly, as well as on giving guidelines and recommendations on how to concretely identify when a processing activity falls into the provision of Art. 22 GDPR and how to concretely ensure the right not to be subject to the decision and to obtain a human intervention.
 - research initiatives and policy makers should investigate solutions specifically thought for AI models, that process personal data by means of machine learning algorithms that may change the logic and the impact on individuals over time, processing personal data of individuals for purposes different or incompatible with the ones for which the data were collected; such solutions could imply data subjects, whose personal data is being processed by means of machine learning algorithms,

²⁰ For more on this, see Consultative Committee of the Convention of the Protection of Individuals with regard to Automatic Processing of Personal Data, *Guidelines on Artificial Intelligence and Data Protection* (25 January 2019), available at: <https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8>.

²¹ For more on this, see UK Information Commissioner's Office, *Big data, artificial intelligence, machine learning and data protection* (4 September 2017), available at: <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>.

²² See Article 22(1) GDPR.

receiving additional information as the AI progresses with its inferences and comes to conclusions.

- **Guidelines on methodology for risk analysis specifically related to AI**, which should take into consideration the circumstances that the risk of the processing, as well as the envisaged consequences for data subjects, may not be comprehensively analysed beforehand by the controller, due to the evolving circumstances of the processing activities.
- **User-friendly instruments to disseminate Ethics guidelines for AI**: need for more user-friendly instruments to disseminate the content of these guidelines, such as Frequently Asked Questions, official disseminating videos, checklists etc

Recommendations from Deliverable D3.5:

Artificial Intelligence

AI, GDPR and Purpose Limitation:

- **It is recommended that limitations or further requirements on the use of personal data within AI-based systems be imposed.** The relevant controller should develop algorithms (and, in particular, machine-learning algorithms) ensuring that personal data is not processed for purposes beyond the scope of their collection (carrying out a compatibility test, where necessary) – **any guidance which can be offered by policy-makers and competent authorities in this regard would prove invaluable.**
- **It is recommended that controllers** should carefully analyse the systems that they wish to implement and **ensure that they are able to provide clear and adequate information to data subjects on how those systems will work and, in particular, the purposes for which they will use personal data** – guidelines or templates on how to disclose such information in a digestible way for individuals (consumers), considering, where relevant, the requirements of Art. 13(2)(f) and 14(2)(g) GDPR, could be of great benefit to AI developers and users.

AI, GDPR and Transparency and Lawfulness

- **It is recommended that guidance and/or means be developed for AI developers and users to provide dynamic information notices** (using illustrations, flowcharts, videos, etc.) to data subjects, seeking to inform them about the **key aspects of how their personal data will be used**, walking them through the AI's process step-by-step and, where relevant, asking for their consent to the parts of the processing which are known at the time. This information and consent request could then be updated/renewed in the case of any foreseen substantial changes at a later stage. However, in order for this to function in a manner similar to the possibility foreseen by Recital 33 GDPR, it is important that the renewal of consent is asked prior to the further processing which relies on it being carried out; this would require **developers to design AI so that it does not automatically proceed with incompatible further processing of personal data, unless it is confirmed – by the developer or user – that a legal basis for this exists.**
- **It is recommended that developers be made aware of the regulations in force and design AI-based systems to allow data pertaining to specific individuals to be extracted from a dataset and not further considered by the system in question.** Guidance and further research on how this can be attained in practice – in particular, considering that, where automated individual decision-making is

concerned, Art. 22(2)(c) GDPR is, as our practical experience has shown, the most likely exception to be relied on – would be welcomed.

AI, GDPR and Security

- **It is recommended further clear and understandable guidelines be developed for AI developers and users on (1) AI risk management, and (2) examples of security measures**, at varying levels of sophistication (to account for developers and users of different sizes, types and economic capabilities), which may be considered in order to properly address identified risks.

Recommendations from Deliverable D3.5:

Recommendations on Artificial Intelligence

- Guidelines on the methodology for risk analysis relating to all levels of risk of AI, aiming at further clarifying the ever-changing aspects of AI.*
- Guidelines on AI/machine learning and data minimisation*
- Provide clarification, through the Artificial Intelligence Act, the tensions between the GDPR principle of purpose limitation and the training and deployment of AI systems*
- Provide guidance on the methodology that SMEs / start-ups training or implementing AI systems in their processes should follow.*
- Guidance and/or other means for AI developers and users to have the ability to provide dynamic information notices (using illustrations, flowcharts, videos, etc.).*
- Guidance around the requirement of traceability as introduced by the High-Level Expert Group on Artificial Intelligence.*
- Provide opportunities to research initiatives, through the Horizon Europe or Digital Europe Program, to explore further ways to grant transparency – for data subjects – on the logic of the automated processing which regards them.*
- Development of further clear and understandable guidelines for AI developers and users on (1) AI risk management, and (2) examples of security measures, at varying levels of sophistication which may be considered to properly address identified risks.*
- Further research and the development of clear, understandable and practical guidelines developing the concept of Fairness by Design (a checklist which could be relied on by AI-based solution developers).*

2.1.7 International Dialogue

The EU Horizon 2020 AEGIS project (Accelerating EU-US Dialogue in Cyberwatching and Privacy) issued a report in June 2018 entitled “Report on Cybersecurity and privacy R&I Priorities for EU-US cooperation. AEGIS Project”²³). AEGIS further the following themes²³ as areas of common interest for EU-US collaboration in the CS&P R&I:

Cyberwatching.eu deliverable D3.3:

Excerpt from “Report on Cybersecurity and Privacy R&I Priorities for EU-US cooperation. AEGIS project.”²³

- The “Top 4 cybersecurity research priorities for EU-US collaboration are Data Security and Privacy, Trust and Privacy, Fight Against Cybercrime and Cybersecurity Education. Among these research domains of common interest for transatlantic collaboration, it is not surprising that **Data security and privacy is**

²³ AEGIS report “Report on Cybersecurity and privacy R&I Priorities for EU-US cooperation” - <http://aegis-project.org/wp-content/uploads/2019/01/AEGIS-Report-on-Cybersecurity-and-Privacy-RI-Priorities-for-EU-US-cooperation.pdf>

seen by more than 80% of the survey respondents as the top research priority in both the US and the EU, given the policy changes in data security and privacy over the past few years. In fact, the EU implemented what are considered to be the world's toughest data protection and privacy regulations, the Directive on the Security of Network and Information Systems (NIS Directive) and the General Data Protection Regulation (GDPR), in May 2018.

- “The Internet of Things is seen as the top priority”
- “Health and Financial Services are overwhelmingly considered the most important sectors to be protected”
- “The cybersecurity and privacy community views the different policies and legislation in the EU and the US as a barrier for collaboration. It’s important to note that although the EU and the US share cybersecurity objectives in policy areas such as public-private information sharing and the creation of international or harmonized cybersecurity standards and policies, collaboration between both regions has not always been easy²⁴. One example of this is the recent implementation in the EU of the NIS Directive and the GDPR, laws that do not have a US equivalent and which caused some US websites to block access to European visitors because they could not comply with the requisites in time²⁵. It’s therefore a logical conclusion that an uneven policy and legislation landscape between both regions can lead to R&I difficulties.”
- “The lack of coordination between funding programs in the US and Europe is also considered an important barrier for R&I collaboration”

2.2 Risk Management

2.2.1 SMEs and information risk management

SMEs often have unique challenges with respect to information risk management. When it comes to information risk management, there is no need to reinvent the wheel; several international reference standards can successfully be used by all players, including SMEs. However, due to multiple factors, specifically, lack of resources and awareness, but also competence and technical capacity to understand and apply standards, many SMEs are simply not in a position to implement sound risk management practices. This situation became more critical during the Covid-19 pandemic. In Deliverable D4.4 “EU Cybersecurity & Privacy Interim Roadmap”²⁶ a set of key challenges facing SMEs, as reproduced below, was provided.

Key challenges for SMEs from Deliverable D4.4:

Challenges facing SMEs:

1. **Lack of awareness.** 69% of European companies have either no or only basic understanding of their exposure to cyber risks²⁷.
2. **Lack of resources.** Most perceive cybersecurity as expensive and lack the necessary resources to adopt adequate security measures. In proportion to their size

²⁴ AEGIS D.1.3 - White Paper on Cybersecurity Policies. Common Ground for EU-US Collaboration, (2018, May 31)

²⁵ Hern, A., & Belam, M. (2018, May 25). LA Times among US-based news sites blocking EU users due to GDPR. Retrieved from <https://www.theguardian.com/technology/2018/may/25/gdpr-us-based-news-websites-eu-internet-users-la-times>

²⁶ Cyberwatching.eu Deliverable D4.4 “EU Cybersecurity & Privacy Interim Roadmap” available online at https://www.cyberwatching.eu/sites/default/files/D4.4_EU-Cybersecurity-%26-privacy-interim-roadmap_v.Final_.pdf

²⁷ Marsh, “Continental European Cyber Risk Survey: 2016 Report,” October 2016, 7 - <https://www.marsh.com/cy/en/insights/research-briefings/continental-european-cyber-risk-survey-2016-report.html>

and income, the investments can be as much as double compared to investments of larger organizations **Error! Bookmark not defined.**

3. **Not only lack of skills and expertise, but also lack of training.** More than 35% of all unfilled vacancies in ICT sector are those of cybersecurity specialists²⁸. There is also a shortage of cyber experts in academia and civil society for educational and training activities. And retaining cybersecurity experts in Europe is another big challenge.
4. **Low uptake of cybersecurity insurance.** Premiums for SMEs are often high and often may not cover some of the prevalent risks, such as losing IP or market share. SMEs therefore may consider cybersecurity investments as inefficient – i.e. costing more than reducing risk²⁹.
5. **Under-reporting of cyber incidents.** Cyber-risks could be handled much easier if early warnings would reach companies on time. However, given the financial repercussions and reputational damage, companies can be reluctant to share information on the number of attacks and the extent of losses incurred, especially companies whose business models are based on trust and privacy³⁰.
6. **Lack of trust.** This is the main inhibitor of cross-sector and cross-border collaboration for SMEs. Intense competition and mistrust of rivals often prevents information exchange and cooperation among different stakeholders. Because of their particular vulnerability, SMEs tend to show a high mis-trust.
7. **Cybersecurity market fragmentation.** The supply of ICT security products and services on the European market is rather fragmented³¹. As a result, even those SMEs that might be willing to adopt cybersecure solutions might need to undergo different certification processes to sell their products and services in several Member States.

One of the ways to overcome such issues is to provide SMEs with specifically tailored (SME-friendly) and easy-to-understand guidelines, which would assist them in navigating their way in the world of advanced methodologies and standards related to information risk management, among which, ISO/IEC 27001 is, without doubt, one of the most solid and affirmed choices.

Bearing this in mind, “The SME Guide for the Implementation of ISO/IEC 27001”³² was developed by a group of SME and cybersecurity experts led by the Chairman Mr. Fabio Guasconi.

²⁸ IDC – Worldwide Skills survey (2017).

²⁹ Study prepared for the European Economic and Social Committee – “Cybersecurity - Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks” - <https://www.eesc.europa.eu/sites/default/files/files/ge-01-18-515-en-n.pdf>

³⁰ Tackling cybersecurity threat information sharing challenges - <https://www.csoonline.com/article/3157540/security/tackling-cybersecurity-threat-information-sharing-challenges.html>

³¹ European Commission (2015), Cybersecurity industry

³² Guasconi F., Sharkov, G., Papadopoulou G., Bulavrishvili, D, et. Al ‘Bulavrishvili’. Brussels: SBS, 2018. Available at: <https://www.digitalsme.eu/digital/uploads/SME-Guide-for-the-implementation-of-ISOIEC-27001-on-information-security-management-min-1-1-1.pdf>

The main principles which, according to these experts, SMEs should follow are the following³³:

- describe an approach that can be used as a first step and upgraded towards a certification
- remove the most "formal" parts of an information security management system
- simplify technical terms used in international standards
- add tips and examples throughout the text
- provide a practical approach towards risk management
- provide sensitive sets of simplified information security controls.

The main steps towards information security risk management, according to the [Guidebook](#), are suggested as follows:

Step 1. Establish information security foundations

- I. Assign roles and responsibilities (top management, information security steering committee, Information security officer/manager, System and information owners, personnel)

Step 2. Understand what must be protected

- I. Identify what information is used
- II. Identify which other assets are used
- III. Understand the connection between information and other assets

Step 3. Evaluate information security risks

- I. Understand the value of assets
- II. Evaluate the type of context in which the organisation works
- III. Identify which controls are already in place

Step 4. Design, apply and monitor information security control

- I. Identify controls to be implemented and set up an Information Security Plan
- II. Manage the Information Security Plan
- III. Control information security
- IV. Monitor information security.

Besides these general guidelines, SME posture could be strengthened by offering technology-specific or sector-specific guidelines on information risk management in concrete areas and building on particular use cases. An example of such is a newly published guide by Digital SME entitled "[SME Guide for Industrial Internet of Things, with Special Focus on Cybersecurity](#)"³⁴.

Recently, ENISA published in June 2021, two publications "Cybersecurity for SMEs – Challenges and Recommendations" and the accompanying Guide "Cybersecurity Guide for SMEs – 12 Steps".

Emerging technologies are opening new market opportunities for SMEs and creating new possibilities to expand their competitiveness, while at the same time they are also raising new vulnerabilities and security risks. Especially during the COVID-19 pandemic, this became clear for the majority of SMEs, who were forced to operate

³³ Fabio Guasconi, 'The SME Guide for the Implementation of ISO/IEC 27001' presentation in cyberwatching.eu webinar 'Cybersecurity risk management: How to strengthen resilience and adapt in 2021', 23 November 2020.

³⁴ Vanetti, M., Mauer, S., Menéndez, F., Tumietto, D., SME Guide for Industrial Internet of Things, with Special Focus on Cybersecurity. Brussels: SBS, 2021. Available at: <https://www.digitalsme.eu/digital/uploads/SBS-SME-Ilot-Guide-2020.pdf>

online, relying on digital technologies as never before, exposing themselves to an ever-growing cyber threats landscape.

When it comes to cyber risks, SMEs and large enterprises are similar in terms of what they can face: cyber-attacks such as data breach, malware and ransomware can happen to all types of organizations. However, while most large businesses have already incorporated cyber risk management into their business strategy, SMEs generally do not regard cyber risk as a strategic component in their business model, as they often lack the awareness, resources or expertise to assess their digital risk exposure and to implement appropriate prevention and remediation measures.

Based on the current context, case studies and past experience, the following good practices for cyber risk management were identified:

- **The human factor is integral to organisational cyber risk management**
Training courses aimed at increasing staff knowledge and awareness of issues such as the use of IT resources and the risks arising from such use are essential in order to prevent and mitigate IT risk. For example, in Italy, only 43.6% of companies state that they provide courses related to IT security³⁵, although the need for such courses is widely recognized.
- **Adopting recognized, official cyber security standards/frameworks is a competitive advantage.**
ISO 27001 is a standard that defines the requirements for setting up and managing an information security management system. The purpose of this certification is to protect data and information by ensuring its integrity, confidentiality and availability. It sets out the requirements for an ISMS aimed at the proper management of sensitive company data. As highlighted in the section above, a very nice initiative for SMEs to get guidance on how to get started on this process is the "[The SME Guide for the Implementation of ISO/IEC 27001](#)"³⁶.
- **Access to privilege controls and administrative rights must be clearly identified.**
Administrative rights, and in general any kind of user rights, means that the holder can take potentially harmful actions, such as:
 - The voluntary or involuntary application of changes that may reduce the level of network security.
 - The introduction of malware that may adopt potentially harmful changes.
 - The theft of access credentials which, with administrative rights, would allow for full use by the abductor.

To increase security accordingly, it is necessary to limit the assignment of administrative rights to what is strictly necessary, ensuring that the privileges assigned are in line with each user's corporate responsibilities and tasks.

An Acceptable Use Policy (AUP) defines the acceptable and unacceptable uses of the company's information resources and IT equipment (computers, wireless devices, telephones, etc.). An appropriate and well-structured policy clarifies the criteria adopted with regard to privacy, user responsibility and personal use of company resources, as well as clarifying the consequences in case of violation. The authorization policies determine the different levels of access to information. An information management

³⁵ Source: "Rapporto clusit 2020"

³⁶ Guasconi F., Sharkov, G., Papadopoulou G., Bulavrishvili, D, et. Al 'Bulavrishvili'. Brussels: SBS, 2018. Available at: <https://www.digitalsme.eu/digital/uploads/SME-Guide-for-the-implementation-of-ISOIEC-27001-on-information-security-management-min-1-1-1.pdf>

system determines whether, when and to which parts of a company's database, the employees are allowed access. These controls define the access to critical information of the company.

- **Vulnerability assessment and remediation plan must be an integral part of the security strategy.**

Vulnerability assessment (VA) is a methodical approach to review security weaknesses in an operating system. aims to bring out all the critical points and possible vulnerabilities of the IT infrastructure and network from a security point of view. The VA ends with a report containing the detected vulnerabilities with their respective severity. Vulnerability assessments should be a periodical exercise for it to be effective as it also fosters operation between security, operations, and development teams. By having at disposal, the data from the VA, SMEs can make informed decisions on how to prioritize limited resources and focus remediation efforts on the areas that can be considered as high priority. The process should be regularly carried out ideally on a monthly frequency.

2.2.2 Cyberwatching.eu Cybersecurity Label

Certification is of high importance to protect businesses (market differentiation, supply chain, etc.) and customers (security by design, etc.), but also because of the Security Industry Policy 2012 that underlined the importance of meeting standards and certification to overcome market fragmentation.

Currently, the certification ecosystem (certification, accreditation, audits, etc.) is a very complex environment from the SME point of view, so there is a need to offer them a clear approach of what they have to do to avoid getting lost during the process. The EU Cybersecurity Act and the different certification schemes that eventually will be implemented will help, but it is still a long and winding road with a great amount of information (schemes, standards, methodologies) to read and process, especially for SMEs.

In cyberwatching.eu, another practical tool has been developed with great potential: the Cybersecurity Label (CL), created by Société Général de Surveillance (SGS) together with the cyberwatching.eu project with the aim of easing the entrance of SMEs into the certification ecosystem. The label represents one of the key SME-facing assets that cyberwatching.eu has provided in order to support SMEs in managing risk. These are described further in Section 5.2. The label addresses in particular which address recommendations outlined in Section 2.1.4: "The cost issue for SMEs looking toward standards and cybersecurity certification must be addressed. SMEs must be able to access standards and the related certification without breaking the bank. Self-assessment and other low-cost solutions must be explored".

The CL is a self-assessment tool for small organizations, either micro/SMEs or startups, that have never had any certification before and which would like to or have to initiate a first contact with a certification scheme.

The label has been co-authored by SGS, the global leader of Testing, Inspections and Verifications and the cyberwatching.eu project. By performing this self-assessment exercise, organizations will have a clear view about the level of security measures they have implemented with respect to a minimum level of security related to the many standards either oriented to systems or security management.

By including a lightweight approach of several and existing certification schemes, this self-assessment exercise includes the security requirements that any organization should comply with in order to demonstrate that it has securely implemented basic logical systems and measures to protect their assets against cyber-threats.

The tool has been developed by an international and reputable company (SGS) with years of expertise in the field of certification, and it is based on a solid approach derived from international standards and best practices.

If an organisation succeeds in the self-assessment, it will obtain the CL as a guarantee of having a reasonable level of security.

The result of the self-assessment also provides a fair impression about the level of protection by identifying the appropriateness of implemented security measures and equipment within the organization.

It allows organizations to go to the cybersecurity consultants of their choice and to provide them with a verified reference that gathers an objective impression of compliance, so that organizations and consulting firms can jointly draft a strategy to implement security measures in accordance with the requirements of more specific standards.

The tool was officially launched in July 2021 at the webinar focused on Standards and Certifications. More information can be found in D3.8 “From research to standardization” and in Section 5.2.2.

2.2.3 Cyberwatching.eu Cyber Risk Temperature Tool

Cyberwatching.eu has also delivered a specific self-assessment tool on risk management. The Cyber Risk Temperature Tool³⁷ is an online self-assessment questionnaire helping SMEs to get a first understanding of the cyber risks threatening their organisation and pave the way for putting in place correct risk assessment processes. The questionnaire consists of two main parts: in the first one, the respondent is asked to give a personal assessment of the company's IT security; while the second part features technical questions.

2.3 Cyberwatching.eu Webinar of July 13, 2021

On July 13, 2021, the Fourth Cyberwatching.eu Concertation Event, took place virtually. During this one-day event, the Horizon Europe (HE) and Digital Europe (DE) programmes presented a new vision and way forward that will shape Europe's digital future.

As the COVID-19 pandemic has shown us, digital technology and infrastructure have a critical role in our private lives and business environments. The EC's Cybersecurity strategy is a commitment to bolstering Europe's collective resilience against cyber threats and helps to ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools.

This Fourth cyberwatching.eu Concertation meeting saw discussions and new partnership opportunities between projects based on the [EU Project Radar](#) and demonstrated results from existing cluster projects formed around market readiness levels and vertical sectors in health, energy and finance.

³⁷ <https://cyberrisk.cyberwatching.eu/Pages/Home.aspx>

With **certification and standardization** a key topic, the event also saw the launch of the cyberwatching.eu Cybersecurity Label and discussion on how emerging technologies are pushing the boundaries of existing privacy regulations.

The main event take-aways are taken from D3.6 “Final Concertation report”.

2.3.1 Horizon Europe and Digital Europe

- Digital sovereignty and autonomy needs to be achieved in Europe. The landscape is very active in this respect with the launch of the Joint Cybersecurity Unit, the EU Competence Centre, and the Cybersecurity Act
- Similarly, these are key themes of the HE and DE. Both build on past activities and it is imperative that proposals should look into results, reuse them and build upon them.
- Proposals should use the Live EU Project radar to see how they can maximise and build on results:
 - Funding on HE topics + related statistics
 - MTRL scores to understand the state of the art
 - Identify results and cite them

2.3.2 Clustering of projects

- Clustering and joint dissemination activities, such as those carried out by cyberwatching.eu which supported over 20 projects, boost sharing of information, education and broader outreach for projects – Projects should use EC services such as Horizon Results Booster to continue support for this. For more details see D2.8 Recommendations report on R&I needs.
- To increase impact of clustering - concrete deliverables or real tasks to generate real outputs are key so all members feel that have a hand in their production
- Exploration of dynamic clustering, pilot synergies including testing and trials, data set sharing, and sharing of threat intelligence

2.3.3 Roadmapping activities

- The competence centre pilot projects have adopted an aligned approach for a common set of research priorities leading to a common roadmap – Technologies, capacity building for a cyber skills framework, building networks
- Continuous public-private dialogue is key for future activities
- Cyber competence network should foster projects and SMEs for a cybersecurity services marketplace

A session at the Concertation Meeting was dedicated to exploring how the four pilot projects that have been running to support the establishment of the European Cybersecurity Competence Centre and Network, what they have researched as Europe’s future cybersecurity priorities and how they have formalized the outcomes into a potential roadmap, and any opportunities or impacts that their conclusions may have for European SMEs. Moderated by Sebastiano Toffaletti of the European DIGITAL SME Alliance, and contributions by Roberto Cascella of ECSO and Edmundas Piesarkas of ReWIRE, each project was given the opportunity to introduce their pilot, the work they had undertaken and the conclusions and outcomes that they have reached as mentioned below (see also further information on the four pilots’ roadmaps in Section 3.4).

CONCORDIA – Cybersecurity cOmpteNce fOr Research and InnovAtion: CONCORDIA identified a series of activities that required synergies from the European Cybersecurity Community, which are: Research and Innovation, Investments, Economics, Standardisation and Certification, and Education and Skills. For each, they identified different short, medium- and long-term activities that required development and collaboration, and suggested ways in which they could be achieved. The CONCORDIA network is a key tool in enhancing the research and education spheres,

as they are providing expertise below the technical level to help develop European capacities.

SPARTA - Strategic programs for advanced research and technology in Europe:

SPARTA also developed a roadmap, based around the cybersecurity technologies that will be required to achieve European digital sovereignty. SPARTA have created an agile and open roadmap, as they believe that a key aspect to ensuring that the roadmap remains relevant and achievable is the flexibility to adapt to new circumstances, technological developments and challenges. The roadmap itself provides a mid-to long term vision of the technological challenges that Europe faces. The roadmap was designed with input from the SPARTA partners, and based on information from the other pilots as well. The Roadmap identifies 13 Mission Projects, which include activities such as certification, Continuous Assessment of Security, IoT Security, Threat Intelligence, AI Technologies etc. These are mapped against a timeline, which provides guidance as to how they can be leveraged for Europe, as well as anticipated challenges in their implementation.

SPARTA also identified research area priorities, based upon the outcomes of the four projects and ECSO’s perspectives. This research is still ongoing, but has already identified four areas:

Focus Area	Examples
Governance and Capacity Building	Collaborative Networks Education and Training Certification
Trustworthy Ecosystems of Systems	Secure Platforms of Platforms Infrastructure Protection
Trust Building Blocks	Holistic data protection AI based security Systems security and Security lifetime management Secure architectures for next-gen communications
Disruptive and Emerging Developments.	Secure Quantum Technologies Secure AI Systems Personalised Privacy Protection

Table 2-1: Research area priorities identified by SPARTA

ECHO - European Network of cybersecurity centres and competence hub for innovation and operations: ECHO’s roadmap is based around 4 pillars:

- technology advancements,
- training and education,
- collaboration (fostered by governance model)
- and certification (focused on products).

ECHO focused the technology roadmap around the use of cyber ranges and is currently developing technology to create a cyber range market place, which can allow for more advanced product testing and modelling. This research led ECHO to suggest that creating a greater market for cybersecurity products and services should be one of the key goals of the Competence Centre, as this will foster the development and uptake of European solutions, particularly those offered by SMEs, thereby enhancing Europe’s digital sovereignty.

Another conclusion that ECHO found is that threat intelligence is one of the key enablers of digital sovereignty, and ensuring that this information is available to companies – not just for security, but for product and service development, should be a priority of national authorities.

Cybersec4Europe - Cyber Security Network of Competence Centres for Europe: with Cybersec4Europe, they focused on seven different application areas to develop roadmaps. This will help contribute to Common Research priorities that has been shared with the JRC and will be part of the Cybersecurity ATLAS.

EC SO: Roberto Cascella explained how EC SO has been working to establish a cybersecurity community working towards a cybersecurity resilient Europe, which is being formalized through efforts towards Europe's digital sovereignty and strategic autonomy. SMEs are a key aspect of this, as they provide the services that can enable this transformation, but at the same time, work needs to be done to ensure that the products and services they offer are cybersecure. To create a Research and Innovation Roadmap, EC SO has consulted the Community, the 4 pilots and then refined the 10 priorities and actions, into short, medium- and long-term goals, working towards 2030.

In the panel discussion, Roberto identified the challenges that Europe – and particularly SMEs – might face in trying to achieve digital sovereignty, which stem from the uncertainty around future priorities and technologies, which is why the roadmaps are important. Identifying the targets and skills required are a key step to achieve digital sovereignty, but ensuring that these build upon existing European competences, rather than creating new ones, so that funding and efforts can leverage already existing capacities – which is a key area for supporting European SMEs as they can bring technologies to vertical sectors.

The expectations of ReWIRE were presented, as this is focused on taking the outcomes from the 4 pilots and turn these into a skills blueprint (as this is an Erasmus+ project, it is heavily focused on skills development) so that European stakeholders can have access to cybersecurity skills materials. These materials will be available for European companies to access.

2.3.4 Standards and certification

- International standards should be (re-)used as much as possible for cybersecurity certification: EU intervention here is key.
- Mapping of standards (and de-facto standards) by EC SO and Concordia are important. However, the standards are in specific areas and don't cover the complex landscape. New standards and systematic effort is needed and a common taxonomy for SMEs
- Standards experts should use EC services and resources such as StandICT.eu³⁸ to contribute to standardization process and contribute to the EC's Open Consultation on Cybersecurity standards.
- New solutions and new funding through HE to further address emerging technologies and CS and privacy challenges - Security and privacy by design are essential concepts
- Clear guidelines or practical tools on data protection for design for emerging technologies like blockchain are required. Cooperation and coordinated approach are needed appropriate methodologies for privacy by design to be implemented.

³⁸ <https://www.standict.eu/>

2.3.5 Support to European SMEs

- European SMEs can be the back bone of EU’s digital sovereignty and autonomy.
- SMEs have high exposure to threats and are often not equipped with the right technical and organisational security to meet legal obligations.
- SMEs shouldn’t be discouraged by the massive and complex amounts of information and procedures.
- Lightweight self-assessment such as Cybersecurity Label³⁹ should whet the appetite for SMEs advance to certification – SMEs need to aim high!
- Certification should drive the growth of the market for SMEs and start-ups, it is a market differentiator for SMEs:
 - trusted, reliable & cost-effective .
 - Affordable (accessible), adapted, aware (adopted) to SMEs.
- Establish trust through standardisation and certification and provide guidance and raise awareness of different assurance levels.
- Tools and solutions need to evolve with the landscape and cannot stay static. They must evolve with the threat landscape.

2.4 Cybersecurity and Privacy R&D ecosystem

To obtain conclusions and suggest recommendations on where it is necessary to invest more efforts to fill the gaps, a quantitative and qualitative analysis was performed in Deliverable D2.8 Recommendations report on R&I needs. The main conclusions are shown below.

2.4.1 Market Readiness Assessment

As explained in Deliverable D2.8, for the **80 projects** that have performed their MTRL self-assessment and obtained a MTRL score, we have been able to determine the maturity of their solutions versus the priorities identified by ECSO in its WG6 in relation with the Security Research and Innovation Agenda (SRIA).

Sorting (low to high) the MTRL scores of these 80 projects for each SRIA priority, we get to the graphic shown in Figure 2-2, where:

- Each circle represents a project addressing that priority (one project can address more than one priority)
- The colours vary from black to green (through red and yellow). Black means lower MTRL score (less mature projects) and green means higher MTRL score (more mature projects).

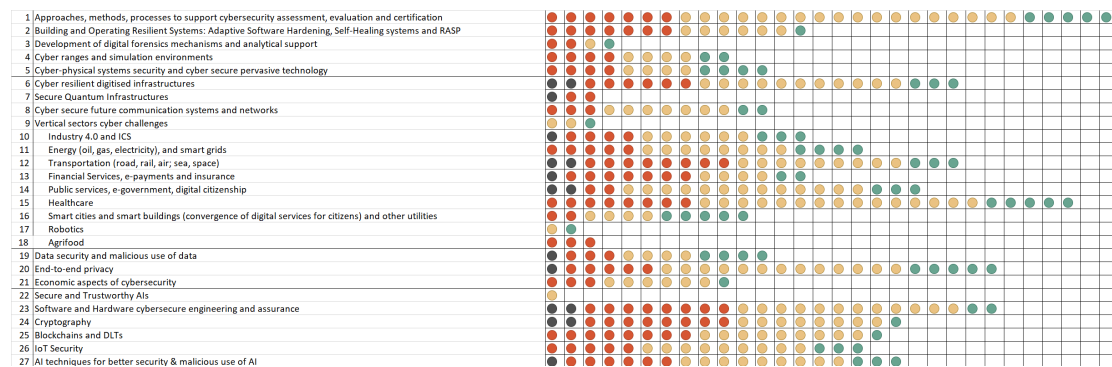


Figure 2-2: Number of projects and its maturity for each priority identified by ECSO

³⁹ <http://gtt.cyberwatching.eu/Pages/Home.aspx>

We can observe that looking only at the average MTRL score, **Secure Quantum Infrastructures** is the less mature priority, while **Robotics** seems to be the more mature priority. Nevertheless, to obtain the “relative maturity” we also need to look at the number of projects addressing each priority. Assigning a weight of 0,5 to the number of projects in each priority and another 0,5 to their average MTRL score, then we get to the following Figure 2-3:

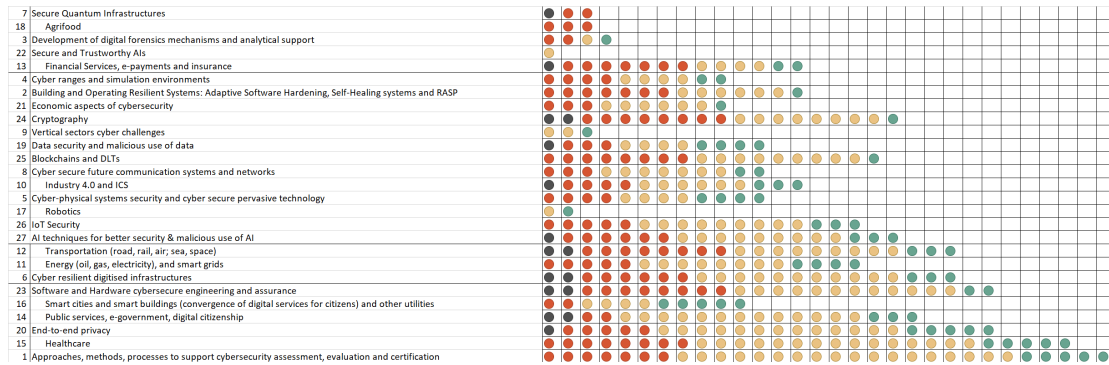


Figure 2-3: Priorities ordered by the average maturity

According to the “relative maturity”, **Secure Quantum Infrastructures** keeps being the less mature priority with only 4 projects in the Project Radar, 3 of them MTRL-assesses and a very low average MTRL score, but **Approaches, methods, processes to support cybersecurity assessment, evaluation and certification** is the more mature priority, with 53 projects in the Project Radar, 30 of them MTRL-assessed, and almost an 80% of them with high maturity.

If we look at the vertical sectors, we could see that Agrifood seems to be the less mature sector and Healthcare the more mature:

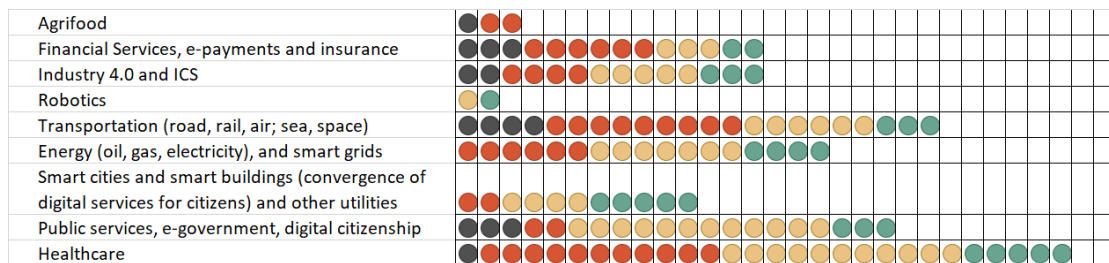


Figure 2-4: Market maturity of cybersecurity solutions from R&D projects by vertical sectors

2.4.2 Identification of low developed spaces

Following the quantitative and qualitative analysis carried out in cyberwatching.eu Deliverable D2.8 “Recommendations report on R&I needs”, a series of conclusions was reached determining where more efforts need to be invested to fill the R&D gaps.

There have been many advances in approaches, methods, processes to support cybersecurity assessment and evaluation, but there is still work to do in **certification**.

There are not many projects working on **self-healing techniques** and their solutions are not very prepared to market yet.

There are not many projects developing **digital forensics** mechanisms and analytical support, and they are not using **AI techniques**.

Cyber ranges play an important role in training and improving the digital capacities, and currently there are not many projects working on these developments, although the maturity of the partial results is not bad.

Projects working on CPS systems are evolving pretty good in closeness to market, but there, but they should keep researching in **information sharing and Meta Attack Language**. The maturity is worse in Cyber resilient digitised infrastructures, as half of the projects are far from market, but **5G and digital twins** are not sufficiently used in this priority.

The priority of **Secure Quantum Infrastructures** is hardly being addressed by projects and the few that exist are not very mature.

The projects working on Cyber secure future communication systems and networks are very mature, but mostly in cloud and IoT, so they need to advance in **5G**.

Regarding Data security and malicious use of data, the projects caring for provenance and integrity of data and assuring data sharing with trusted third parties are pretty mature. But there are no projects working on **fake news**.

There are many projects working on End-to-end privacy, mainly focused on GDPR compliance, privacy-preserving and data leakage, and most of them are mature.

Some projects are just focusing on the economic aspects of cybersecurity and other are integrating this analysis as part of the projects, either analysing the economic impact of cyber-threats or assessing business models for their solutions. Most of them are not so far from the market.

Just a couple of projects are researching on the **threats related to using AI**, and they are not mature.

More and more projects are taking into account security and privacy by design, and there are a few tools that help developers to do the same. Nevertheless, not all are mature enough, and only 50% are relatively close to market.

There are many projects using cryptographic techniques within their projects, but there are not so many projects researching specifically on cryptography. Again, not all are mature enough, and only 50% are relatively close to market.

Despite the fact that the blockchain is a technology that has been researched for years, it is not fully implemented globally. Most projects use blockchain as a mean to reach the goals of their projects, but not as the main focus of their projects, and only 50% are relatively close to market.

A few projects focus on security for IoT devices, although they are pretty mature. Not many mention **anonymisation**.

Artificial intelligence is increasingly widespread, by using Machine learning, Deep learning and even Reinforcement learning, for threat analysis, predictive analysis and information sharing, and presents more projects near the market than far.

2.5 Recommendations to EU on Projects

After the clustering activities with R&D projects and the performed gap analysis, cyberwatching.eu is in the position to give some recommendations to EC.

The first part of the recommendations comes from the identification of low developed spaces, and therefore they are oriented to cover the gaps.

The second part of the recommendations comes directly from 17 engaged projects that participated in a survey regarding their main interests.

2.5.1 Recommendations from Cyberwatching.eu

The following are a set of recommendations from Deliverable D2.8 (July 2021).

R1. Give value to the results of projects already developed, not only forcing to incorporate a section on previous initiatives in the Horizon Europe proposals, but also promoting among organisations the different tools that allow consulting and taking advantage of the results of previous projects, such as the Cyberwatching.eu Project Radar⁴⁰, the Horizon Results Platform⁴¹ or the Horizon Result Booster⁴².

R2. Promote clustering activities as a way to encourage collaboration between projects, joint dissemination and exchange of good exploitation practices, including the possibility of joint exploitation or joint future developments.

R3. Encourage projects to do intermediate self-evaluations, beyond the mandatory reviews with the EC, to check that their project is progressing correctly at the technological and market level. The self-assessment should be done by the same person in the project.

R4. Promote activities for projects related to developing skills in areas like Go to market and the Manufacturing/Supply chain, such as helping them to get in contact with potential clients and partners, so that they can adapt the results of the projects to the real needs of the consumers and can establish commercial relationships.

R5. Robotics and agrifood should be considered as preferred sectors for pilots and use cases.

R6. Industry 4.0 could also be a recommended sector for pilots, due to the priority of digital transformation by companies.

R7. Research in Secure and Trustworthy AIs must be encouraged, considering the growing use of AI for improving cybersecurity and privacy.

R8. Development of certification schemes and standards should be encouraged.

R9. Cyber ranges have to continue to be promoted and improved their market maturity,

R10. Information sharing and Meta Attack Language in CPS systems should be further researched.

R11. 5G and digital twins should be further researched in Cyber resilient digitised infrastructures. Also, 5G has to be researched in Cyber secure future communication systems and networks.

⁴⁰ <https://radar.cyberwatching.eu/radar>

⁴¹ <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-results-platform>

⁴² <https://www.horizonresultsbooster.eu/>

- R12.** Secure Quantum Infrastructures has to be intensively promoted.
- R13.** Regarding Data security and malicious use of data, research in fighting fake news should be carried out.
- R14.** Research on threats related to using AI should be highly encouraged.
- R15.** Research on new and advanced cryptographic techniques should improve their maturity.
- R16.** Blockchain should be integrated in cross- border and cross-domain settings.

Table 2-2: Cyberwatching Recommendations - EU Projects

As reported in Section 2.2.1, the human factor is integral to organisational cyber risk management for SMEs. However, the RI pipeline of research projects on this topic is emptying.

Deliverable D2.7, reports that based on the current live version of the EU project radar, the topic of Human Aspects and Identity & Privacy was an overrepresented sector for research projects in 2018. Now though, 84% of these projects are now completed and this has become significantly the smallest areas of active projects, with only two projects that are ongoing within the radar. Given the increasing popularity of social engineering in cybersecurity incidents, it is somewhat surprising that we are now in this situation with the projects as assessed as one should consider that within the CS & P landscape. “Human Aspects of Cybersecurity” is the one sector in the radar that most clearly represents fundamental research. Unfortunately, as we had previously identified this most fundamental factor of effective cybersecurity appears to still be orphaned.

As many of the most pressing cybersecurity and privacy issues are fundamentally socially based, **we consider that the long-term funding strategy for cybersecurity and privacy must put more focus on Human Aspects, and Identity and Privacy, and less focus on technical solutions addressing the same issue since this area is already heavily supported.** This is of particular concern with the newly announced Horizon Europe Cybersecurity calls all being technology focused meaning that there is likely to be a point in the near future where there are no funded actions that are dealing with human aspects at all. This will mean that there is a gap in the availability to new projects of outputs that may no longer be at the cutting edge when compared to other domains.

2.5.2 Recommendations gathered from other EU projects

During the course of the project, Cyberwatching.eu collected **recommendations from the engaged projects** regarding measures that EC could apply to minimize the barriers for the commercialization of the projects results. The main recommendations are presented below.

- Support, Intellectual property, Business Skills, Communication/Dissemination, R&D.
- Make GDPR compliance easier for small enterprises (Start-ups and SMEs), that usually do not have the strength or the knowledge to understand what they shall do to be compliant.
- Collaboration between peer projects should be promoted by the EC.
- The EC should provide more resources to address privacy awareness issues.
- EC should promote EU-based solutions.
- Push for a special treatment of cybersecurity budgets, such as Cybersecurity 4.0

- Foster and coordinate standardization efforts towards new generation of cybersecurity systems, which leverage the collaboration between providers of digital services and infrastructures.
- Promote and foster the adoption of security capabilities as extensions to existing interfaces and APIs.
- Promote the adoption of certification schemes and award those providers that give visibility of security features in their products.
- Ease the access to EU administration/LPA decision makers.
- Foster the use of eID by the citizenship.
- More standardisation and common frameworks are needed to be adopted on IoT applications which are dispersed “silos” so far, and even more on Security / Cyberthreat common standards. EC could support with joint efforts on a common/standardised framework adopted by all “big players.”
- Improve the investment in continuous human resource training to facilitate the uptake of innovative solutions.

2.6 Summary of recommendations from Cyberwatching.eu Project

In summary, the [cyberwatching.eu](https://www.cyberwatching.eu) project work efforts have resulted in a number of different recommendations in multiple cybersecurity domains, which essentially represent a roadmap of key important points that need to be addressed now and into the future. Table 2-2 to Table 2-6 presents the recommendations gathered through the project according to area of recommendation, an indication of the type of action required, with further details of the recommendation or area for research.

GDPR - Data Protection – Regulatory Framework	
Type of need	Description of Recommendations / Research / Explicit Need
Guidelines / Clarification Research	<p>Clarifications on the intricacies between GDPR and NIS:</p> <ul style="list-style-type: none"> ○ DEP could use industry to shed light on the procedures that take place in real time of such circumstances, and the research component (Horizon Europe) should find the most time-efficient and compliant method of managing notifications that fulfill the requirements of both the NIS Directive and the GDPR ○ Policy-makers could provide guidance for organisations on the extent to which sanctions will be applied for both legislations and how such violations will be regarded by competent authorities and member states.
Guidelines	<p>Practical clarifications on the application of the GDPR to blockchain are very much needed for this technology and the law to coexist. It should be clarified how those systems could be specifically crafted, in careful consideration of the rules set by the principles of data protection by design and, specifically, of fairness by design, to ensure that individuals' privacy and real control over their data is afforded to them:</p> <ul style="list-style-type: none"> ○ While some principles remain largely unaffected by the technology, such as the principle of lawfulness and purpose limitation, and others may even find themselves enhanced by the additional functionalities brought about by blockchain, such as the principle of fairness, others still appear to frontally collide with its 'set-in-stone' nature, namely the principles of data minimisation and storage limitation which, in turn, may affect the ability to effectively exercise some data subject rights regarding personal data stored 'on-chain' (such as the right to rectification or erasure). ○ It is also not a simple matter to identify and agree on the data processing roles played by the participants in a blockchain-based system. ○ An even more complicated matter is to ensure that the formal requirements tied into these roles are met, such as the need for a contract or other legal act containing a set of minimum obligations to be entered into with each processor engaged by a controller, in light of Art. 28 GDPR – this problem currently appears not to have a practically viable solution when considering public blockchains. ○ The matter of international transfers and the implementation of the requirements for their lawfulness raises similar difficulties in light of the decentralised nature of blockchain-based systems.
Methodology	<p>Publication of a systematic Methodology for GDPR risk assessments which will be available for all stakeholders in every Member State.</p>
Methodology / Guidelines	<p>Guidelines on methodology for risk assessment especially focused on each sector of the OES (NIS Directive) – which are essentially the critical infrastructure of countries: ENISA could work together with the DEP stakeholders, with the aim of producing practical guidelines for assessing the risks in the essential services of member states at a centralised European level.</p>
Methodology	<p>Updated methodology to assess the severity of data breaches and feedback on tool for notification of data breaches: there is a need for further guidelines on the assessment of the severity of breaches and a</p>

GDPR - Data Protection – Regulatory Framework	
Type of need	Description of Recommendations / Research / Explicit Need
	methodology on how to manage and react to the breaches. This recommendation could be achieved by updating of the existing methodology from ENISA.
Guidelines	Allocation of specific priority areas that require instruments or guidance to different Supervisory Authorities, in order to ensure efficiency and consistency in the guidance provided to organisations.
Guidelines	Publication of guidelines and recommendations on Data Transfer Impact Assessment .
Tool / Platform / Guidelines	Creation of a data transfer impact assessment , which will assist organisations to assess all relevant factors and considerations before carrying out data transfers outside the EEA.
Guidelines	Need for further guidelines on the application of principles of data protection by design/default and data minimisation for IoT deployments: such guidelines should give advice on how to concretely inform users as per Art.s 12-13-14 GDPR, which legal basis is permitted to process personal data and how data subjects can effectively exercise their rights. Moreover, such guidelines should address end-to-end security during the entire data-lifecycle, given that the machines performing data processing are typically under the control of different organisations (acting as controllers or processors as the case may be) without an overarching orchestration and control over the data.
Guidelines	Practical guidelines on the allocation of privacy roles in IoT environments in the light of the GDPR are needed, since IoT poses strong challenges to the allocation of privacy roles of the several parties involved in processing. The use of data protection contracts (i.e., Privacy Level Agreements) - other than data processing agreements pursuant to Art. 28 or joint-controllership agreements pursuant to Art. 26 GDPR – should be considered, whereby, regardless of the privacy rules, duties, obligations and responsibilities of the parties involved are clearly spelled out.
Tool / Online Platform	Creation of a single space to collect all the different types of guidance (opinions, guidelines, instruments, tools, self-assessments) created by Supervisory Authorities based on the GDPR ‘topic’ or GDPR ‘obligation’ to ensure easy access availability.
Tool	European tool for Data Protection Impact Assessment: the creation of a tool for data protection impact assessments, which could compile the several applicable national black lists, is highly recommended.
Tool	European self-assessment tool: it is recommended that the EC invests in research initiatives in order to create a tool, or several ones, that can serve as more practical instruments to increase the compliance of all organisations (multinationals, medium, small and micro enterprises, research projects) under the scope of the GDPR. (1, 2, 3)
Research and Guidelines	Guidance on implementation of data protection by design and by default in emerging technologies: further research and guidance on How privacy by design and by default can be involved in industry standards for emerging technologies is highly recommended.
Research	Further research on managing notifications that fulfill the requirements of both the NIS Directive and the GDPR.
Ethics	Encouraging the creation of codes of conduct to demonstrate compliance: It is recommended that in the context the DEP’s objectives

GDPR - Data Protection – Regulatory Framework	
Type of need	Description of Recommendations / Research / Explicit Need
	the European Commission encourages the creation of codes of conduct, pursuant to art. 40 GDPR; these codes of conduct should take into account the specific features of the processing sectors as well as the specific needs of micro, small and medium-sized enterprises.
Research / Tools / Instruments	European certifications, seals and marks on data protection: the European Commission shall encourage, in particular at the European level, the establishment of data protection certification mechanisms and data protection seals and marks described in articles 42 GDPR. For this purpose, there is a need for a strategic research initiative which will propose a structured approach to certify tools and other instruments created by private entities as compliant at European level.

Table 2-3: Cyberwatching Recommendations - Legal Aspects

Standards and Certification	
Type of need	Description of Recommendations / Research / Explicit Need
Education	EC funding for Raising Awareness and Education in Cybersecurity Standards and Certification for both the Public and Private sectors. This recommendation stems from the repeated request in a Cyberwatching.eu survey, and at events, to provide information, education and guidance so that both public and private sectors in order to move forward with the essential knowledge to address this gap of expertise in standards and certification. It is already recognised that Europe does not have enough of skilled experts which the industry needs and stakeholders lack the cybersecurity knowledge.
Education / Research	Education and training to raise industry awareness: research initiatives should find the best method to educate the industry operating in the field of emerging technologies on ways to address the existing challenges and give practical instructions on how to concretely achieve compliance.
Policy	The issues of Mutual Recognition and Harmonisation must be addressed due to the national nature of many standards and certification systems
Education & Training	Further efforts must be made in order to raise awareness concerning the available accepted standards and certification , as well as the certification process in case of multi-party composition of products and solutions
Policy / Education	International Cooperation is an area for opportunities to benchmark best practices and standards that may already exist as a way to not “reinvent the wheel”, however, caution is urged in taking care not to immediately co-opt existing standards that may put European industry at a disadvantage. From the results of ongoing projects in US and JP, several common areas of interest for collaboration emerged
Cost effective solution	The cost issue for SMEs looking toward standards and cybersecurity certification must be addressed. SMEs must be able to access standards and the related certification without breaking the bank. Self-assessment and other low-cost solutions must be explored.
Research	The R&I community should look address the fast-evolving area of Internet of Things (IoT) with respect to cybersecurity standards and certification.

Standards and Certification	
Type of need	Description of Recommendations / Research / Explicit Need
	The lack of cybersecurity standards and certification in IoT requires some concerted effort on the part of the research and industrial community to address this fast-evolving gap. This is also a well-known area that will be on the agenda of organisations such as the IoT Forum and ECSO
Research	Elaborate a common research agenda across EU Member States (MS). Through the vehicle of the ERC which is available to all MS scientists, it would be sensible to open out specific calls for projects in the area of cybersecurity with clear aims and requirements on developing in areas of relevance to standards in cybersecurity. This call should be preceded by a large publicity campaign. It would not be possible to get MS themselves to operate internal funding in a coherent manner so using academic research focused central money such as ERC would be a more cost-effective mechanism. There should also be the continued push for EC sponsored research to be fully open access not only in the final publication but also in the protocols, software and data used within the projects supported.

Table 2-4: Cyberwatching Recommendations – Standards and Certification

Emerging Technologies, IoT		
Type of need	Recommendations / Research / Explicit Need	JRC Cybersecurity Domains
Guidelines	Practical guidelines on compliance of automated processing in the context of emerging technologies: The DEP can prioritise to give guidance on how to demonstrate compliance where the automated processing activities may not be possible or easy to disclose in information notices.	
Policy Guidelines /	Structured cooperation between policy makers, the research and the market/industry: the DEP should aim at drafting a structured flow of information that facilitates the continuous sharing of feedback between policy makers, research initiative and industry on matters regarding emerging technologies.	
Guidelines	Guidelines on anonymisation tools and pseudonymisation mechanisms: it is recommended that the European Commission stimulates the creation of guidelines on anonymisation and pseudonymisation mechanisms, which are acceptable as being able to address the challenges of emerging technologies.	
Tools	Creation of practical tools focusing on compliance of emerging technologies, that are kept up to date according to the industry standards and state of art as well as rate of change of the technologies.	
Education	Education and training to raise industry awareness in the field of emerging technologies.	
Cooperation / Policy	Structured cooperation between policy makers, the research and the market/industry.	
Guidelines	Need for further guidelines on the application of principles of data protection by design/default and data minimisation for IoT deployments: such guidelines should give advice on how to concretely inform users as per Art.s 12-13-14 GDPR, which legal basis is permitted to process personal data and how data subjects can effectively exercise	

Emerging Technologies, IoT		
Type of need	Recommendations / Research / Explicit Need	JRC Cybersecurity Domains
	<p>their rights. Moreover, such guidelines should address end-to-end security during the entire data-lifecycle, given that the machines performing data processing are typically under the control of different organisations (acting as controllers or processors as the case may be) without an overarching orchestration and control over the data.</p>	
Guidelines	<p>Practical guidelines on the allocation of privacy roles in IoT environments in the light of the GDPR are needed, since IoT poses strong challenges to the allocation of privacy roles of the several parties involved in processing. The use of data protection contracts (i.e., Privacy Level Agreements) - other than data processing agreements pursuant to Art. 28 or joint-controllership agreements pursuant to Art. 26 GDPR – should be considered, whereby, regardless of the privacy rules, duties, obligations and responsibilities of the parties involved are clearly spelled out.</p>	
Methodology	<p>IoT and Data Minimisation</p> <ul style="list-style-type: none"> It is recommended that IoT developers/providers consider to more comprehensively design IoT devices and services with the principle of data minimisation in mind, incorporating the concepts of data protection by design and by default into the development process. In particular, as has been noted by the Article 29 Data Protection Working Party in the past, the principle of data minimisation “<i>specifically implies that when personal data is not necessary to provide a specific service run on the IoT, the data subject should at the least be offered the possibility to use the service anonymously</i>”. 	
Tool	<ul style="list-style-type: none"> One of the ways in which this could be done, which would also address the problem of individuals’ lack of control over IoT data flows, would be for developers to consider creating ‘privacy dashboards’ or ‘privacy interfaces’ for individuals – these dashboards/interfaces, which could be available on specific devices (such as an individual’s mobile phone), could act as a control centre for that individual’s IoT devices and services, offering information and options concerning data receipt and transmission for each device or service. 	
Policy	<ul style="list-style-type: none"> It is recommended for Controllers to consider if this problem which could be addressed by policy and regulation, where stricter requirements on data collection and transmission could be enforced on IoT developers. Possible solutions could include an obligation to build in ‘do not collect’ switches or permissions into IoT devices and services, so that individuals can disable or limit collection and transmission of data before even activating the device or service. 	

Emerging Technologies, IoT		
Type of need	Recommendations / Research / Explicit Need	JRC Cybersecurity Domains
<p>Tool</p> <p>Policy</p>	<p>IoT and Purpose of limitation:</p> <ul style="list-style-type: none"> The imposition of limitations or further requirements on subsequent processing of personal data, collected and shared between IoT-connected devices and services, seems to be a reasonable solution. It is recommended to provide individuals with control over which data may be collected and transmitted, through the use of dashboards, privacy centres or other privacy enhancing technologies, - this would already be a large step to achieve this goal. It is recommended that contractual limitations between stakeholders (through Data Management Agreements) be imposed on the further processing of received personal data as this could be a key step in ensuring that appropriate limitations are in place, particularly in the absence of stricter and clearer policy on IoT data collection, sharing and repurposing. 	
Tools	<p>IoT and Transparency and lawfulness:</p> <ul style="list-style-type: none"> Two suggestions to help comply with the principle of transparency are the use of just-in-time notifications and periodic notifications, which may allow developers to deliver specific and relevant information to individuals at times when they are most likely to be able to apprehend such information. Furthermore, as noted above, the development of privacy dashboards or control centres for individuals may be fundamental in this respect, as it can allow not only the creation of a central point where information on the processing activities undertaken may be accessed, but also where individuals may set their preferences in regards to data collection/transmission and, potentially, also exercise their rights under the GDPR directly (e.g., accessing, rectifying, deleting or exporting personal data captured by IoT-connected devices). It is recommended that further research continue and guidelines be produced on effective means by which information on processing activities carried out via IoT can be delivered to individuals – particularly those who may be captured by the sensors of such devices, without necessarily owning them or having activated them (such as visitors or passers-by). 	
<p>Guidelines</p> <p>Methodology</p> <p>Guidelines</p>	<p>IoT Security:</p> <ul style="list-style-type: none"> It is recommended that further research continue and the development guidelines and procedures be developed to assist controllers in carrying out regular monitoring and testing activities, when faced with systems composed of multiple IoT-connected devices. Furthermore, an additional consideration would be the implementation of end-to-end encryption regarding all data collected and transmitted by and between IoT-connected devices and services. 	

Emerging Technologies, IoT		
Type of need	Recommendations / Research / Explicit Need	JRC Cybersecurity Domains
	<ul style="list-style-type: none"> It is recommended that further security measures and best practices which should be considered include those within ENISA's guidelines on Good Practices for Security of Internet of Things. 	
Guidelines	<p>IoT:</p> <ul style="list-style-type: none"> Need for further guidelines on the application of principles of data protection by design/default and data minimisation for IoT deployments. Practical guidelines on the allocation of privacy roles in IoT environments in the light of the GDPR. Guidance or further research into the key aspects to be regulated between stakeholders, via Data Management Agreements (in particular, where the controller-to-controller terms are concerned), to provide tools for stakeholders to effectively self-regulate. Impose limitations or further requirements on subsequent processing of personal data, collected and shared between IoT-connected devices and services. Guidelines on effective means by which information on processing activities carried out via IoT can be delivered to individuals – particular those who may be captured by the sensors of such devices, without necessarily owning them or having activated them (such as visitors or passers-by). Guidelines and procedures to assist controllers in carrying out regular monitoring and testing activities, when faced with systems composed of multiple IoT-connected devices. Ensure that IoT developers and users are bound by ethical considerations in their activities, further research and the development of clear, understandable and practical guidelines developing the concept of Fairness by Design (including, for example, a checklist which could be relied on by IoT-based solution developers) would be welcomed. 	
Guidelines		
Policy		
Guidelines		
Policy		
Guidelines		
Guidelines		
Ethics		

Table 2-5: Cyberwatching Recommendations - Emerging Technologies, IoT

Artificial Intelligence		
Type	Recommendations / Research / Explicit Need	JRC Cybersecurity Domains:
Guidelines	<p>Guidelines on AI/machine learning and data minimisation: it is recommended that policy makers strive for research initiatives that look into how to concretely deploy AI and machine learning models, respect the principle of data minimization, storage limitation and data accuracy (Article 5 (1) (b), (c), (d) GDPR).</p>	
Research		
Research	<p>Solutions to address complexity of processing in the context of AI and principle of transparency:</p> <ul style="list-style-type: none"> it is recommended to invest in researching initiatives which aim at focusing on how to safeguard and ensure transparency when the complexity of emerging technologies escalates constantly, as well as on giving guidelines and recommendations on how to concretely identify when a processing activity falls into the provision of Art. 22 	

Artificial Intelligence		
Type	Recommendations / Research / Explicit Need	JRC Cybersecurity Domains:
	<p>GDPR and how to concretely ensure the right not to be subject to the decision and to obtain a human intervention.</p> <ul style="list-style-type: none"> research initiatives and policy makers should investigate solutions specifically thought for AI models, that process personal data by means of machine learning algorithms that may change the logic and the impact on individuals over time, processing personal data of individuals for purposes different or incompatible with the ones for which the data were collected; such solutions could imply data subjects, whose personal data is being processed by means of machine learning algorithms, receiving additional information as the AI progresses with it inferences and comes to conclusions. 	
Guidelines / Methodology	<p>Guidelines on methodology for risk analysis specifically related to AI, which should take into consideration the circumstances that the risk of the processing, as well as the envisaged consequences for data subjects, may not be comprehensively analysed beforehand by the controller, due to the evolving circumstances of the processing activities.</p> <p><i>Guidelines on the methodology for risk analysis relating to all levels of risk of AI</i>, aiming at further clarifying the ever-changing aspects of AI.</p>	
Tools	<p>User-friendly instruments to disseminate Ethics guidelines for AI: need for more user-friendly instruments to disseminate the content of these guidelines, such as Frequently Asked Questions, official disseminating videos, checklists etc.</p>	
Guidelines	<p>AI, GDPR and Purpose Limitation:</p> <ul style="list-style-type: none"> It is recommended that limitations or further requirements on the use of personal data within AI-based systems be imposed. The relevant controller should develop algorithms (and, in particular, machine-learning algorithms) ensuring that personal data is not processed for purposes beyond the scope of their collection (carrying out a compatibility test, where necessary) – any guidance which can be offered by policy-makers and competent authorities in this regard would prove invaluable. It is recommended that controllers should carefully analyse the systems that they wish to implement and ensure that they are able to provide clear and adequate information to data subjects on how those systems will work and, in particular, the purposes for which they will use personal data – guidelines or templates on how to disclose such information in a digestible way for individuals (consumers), considering, where relevant, the requirements of Art. 13(2)(f) and 14(2)(g) GDPR, could be of great benefit to AI developers and users. 	
Guidelines / Tools /	<p>AI, GDPR and Transparency and Lawfulness</p> <ul style="list-style-type: none"> It is recommended that guidance and/or means be developed for AI developers and users to have the ability to provide dynamic information notices (using illustrations, flowcharts, videos, etc.) to data subjects, seeking to inform them about the key aspects of how their personal data will be used, walking them through the AI's process step-by-step and, where relevant, asking for their consent to the parts of the processing which are known at the time. This 	

Artificial Intelligence		
Type	Recommendations / Research / Explicit Need	JRC Cybersecurity Domains:
Policy	<p>information and consent request could then be updated/renewed in the case of any foreseen substantial changes at a later stage. However, in order for this to function in a manner similar to the possibility foreseen by Recital 33 GDPR, it is important that the renewal of consent is asked prior to the further processing which relies on it being carried out; this would require developers to design AI so that it does not automatically proceed with incompatible further processing of personal data, unless it is confirmed – by the developer or user – that a legal basis for this exists.</p> <ul style="list-style-type: none"> It is recommended that developers be made aware of the regulations in force and design AI-based systems to allow data pertaining to specific individuals to be extracted from a dataset and not further considered by the system in question. Guidance and further research on how this can be attained in practice – in particular, considering that, where automated individual decision-making is concerned, Art. 22(2)(c) GDPR is, as our practical experience has shown, the most likely exception to be relied on – would be welcomed. 	
Guidelines	<p>AI, GDPR and Security <i>It is recommended further clear and understandable guidelines be developed for AI developers and users</i> on (1) AI risk management, and (2) examples of security measures, at varying levels of sophistication (to account for developers and users of different sizes, types and economic capabilities), which may be considered in order to properly address identified risks.</p>	
Policy	Provide clarification, through the Artificial Intelligence Act , the tensions between the GDPR principle of purpose limitation and the training and deployment of AI systems	
Guidelines / Methodology	Provide guidance on the methodology that SMEs / start-ups training or implementing AI systems in their processes should follow.	
Guidelines / Policy	Guidance around the requirement of traceability as introduced by the High-Level Expert Group on Artificial Intelligence.	
Research	Provide opportunities to research initiatives , through the Horizon Europe or Digital Europe Program, to explore further ways to grant transparency – for data subjects – on the logic of the automated processing which regards them.	
Guidelines	Development of further clear and understandable guidelines for AI developers and users on (1) AI risk management, and (2) examples of security measures, at varying levels of sophistication which may be considered to properly address identified risks.	
Research Guidelines	Further research and the development of clear, understandable and practical guidelines developing the concept of Fairness by Design (a checklist which could be relied on by AI-based solution developers).	

Table 2-6: Cyberwatching Recommendations - AI

3 Roadmaps from European and international sources

3.1 EU Cybersecurity Strategy

The key elements of the Cybersecurity strategy that in principle consists of four elements

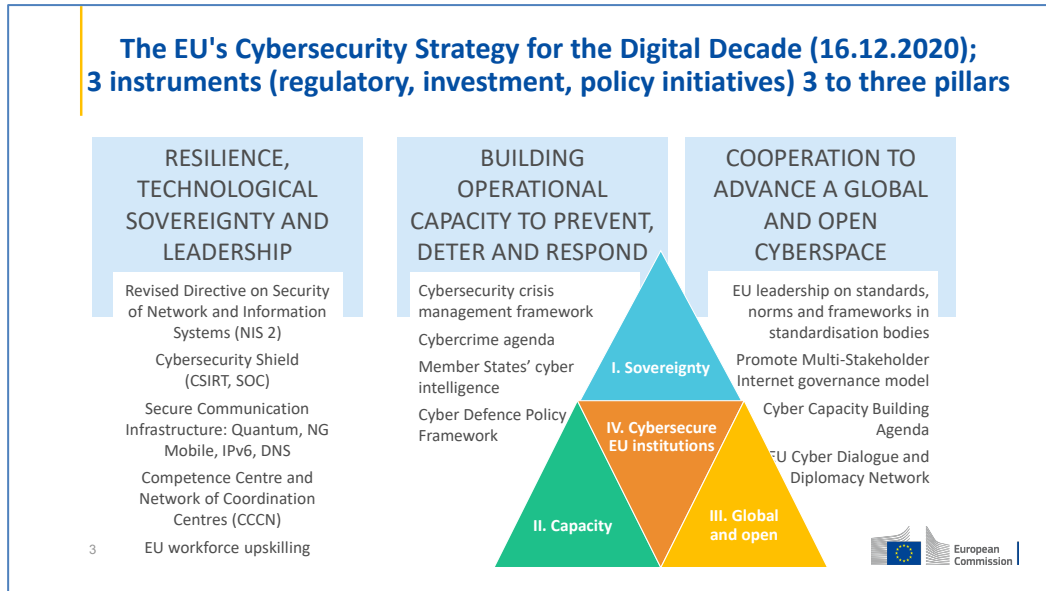


Figure 3-1: EU Cybersecurity Strategy⁴³

The **EU Cybersecurity Strategy**⁴⁴ describes how the EU can harness tools and resources to become technically sovereign. It covers the next 7-year funding period and deploys regulatory, investment and policy initiatives across three areas of action:

1. resilience, technological sovereignty and leadership;
2. operational capacity to prevent, deter and respond;
3. cooperation to advance a global and open cyberspace.

3.1.1 Resilience, technological sovereignty and leadership

This includes the proposal for a revised Directive on Security of Network and Information Systems (NIS 2 Directive). The Commission proposal expands the scope of the current NIS Directive by adding new sectors based on their criticality for the economy and society, and by introducing a clear size cap – meaning that all medium and large companies in selected sectors will be included in the scope. At the same time, it leaves some flexibility for Member States to identify smaller entities with a high security risk profile.

The Commission also proposes to launch a network of Security Operations Centres across the EU, powered by artificial intelligence (AI), which will constitute a real 'cybersecurity shield' for the EU, able to detect signs of a cyberattack early enough

⁴³ Slide taken from presentation of Monika Lanzenberger, DG Connect, European Commission presenting "Cybersecurity in Horizon Europe & Digital Europe" at the Cyberwatching Online Concertation event available at: https://www.cyberwatching.eu/sites/default/files/Cybersecurity%20in%20Horizon%20Europe%20Digital%20Europe_20210713.pdf

⁴⁴ The EU Cybersecurity Strategy online at <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy>

and to enable proactive action, before damage occurs. This builds on top of the CSIRTs includes a reference to the Security Operating Centres.

3.1.2 Operational capacity to prevent, deter and respond

This covers the Joint Cybersecurity Unit which will provide a virtual and physical platform for cooperation for the different cybersecurity communities in the EU. It will focus on operational and technical coordination against major cross-border cyber incidents and threats. An assessment of the JCU organisational aspects and an identification of EU operational capacities will be published by the end of 2021 while by June 2022 and incident and response plan will be published. This will be operational by the end of 2022 and expanded to industry by June 2023.

3.1.3 Cooperation to advance a global and open cyberspace

This element covers standards and international cooperation and establishing EU leadership on standards. The Cybersecurity Act is a key element here which came into force in 2019. The EC is currently working on a Union ROLLING Work Programme for Cybersecurity Certification which will be published in late 2021. The cybersecurity framework will feature one framework covering a broad scope which includes products, services and processes as well as an inclusive and transparent governance process which includes the ECCG (European Cybersecurity Certification Group) which is composed of representatives of national cybersecurity certification authorities or representatives of other relevant national authorities; and the SCCG (Stakeholder Cybersecurity Certification Group) which represents cybersecurity experts and advises the Commission and ENISA, the European Union Agency for Cybersecurity, on strategic issues regarding cybersecurity certification.

3.1.4 European Data Strategy

The [European Data Strategy](#) sets out how European can promote its data market and data economy through promoting fair, accessible data that respects individuals privacy. Roadmap for:

- setting clear and fair rules on access and re-use of data
- investing in next generation tools and infrastructures to store and process data
- joining forces in European cloud capacity
- pooling European data in key sectors, with common and interoperable data spaces
- giving users rights, tools and skills to stay in full control of their data

[European Data Strategy \(Regulation on data governance\)](#) – regulation will help boost data sharing across Europe through regulating data spaces.

3.2 European Agency for Network and Information Security (ENISA)

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union in cooperation with the wider community. It does this through acting as a centre of expertise on cybersecurity, collecting and providing independent, high quality technical advice and assistance to Member States (MS) and EU bodies on cybersecurity. It contributes to developing and implementing the Union's cyber policies.

3.2.1 ENISA 2020 Strategy

The ENISA 2020 Strategy - a Trusted and Cyber Secure Europe, sets out the objectives that will drive ENISA's work in the coming years to meet the many challenges ahead. The document identifies 7 Strategic objectives

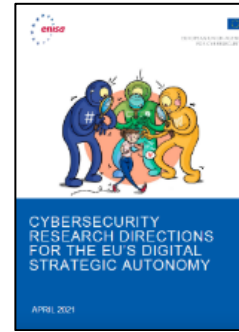
Strategic objective & context	Target achievements
-------------------------------	---------------------

<p>Empowered and engaged communities across the Cybersecurity ecosystem: Cooperation across stakeholders, MSs and institutions.</p>	<p>An EU-wide state of the art body of knowledge to build cooperation and expertise. An empowered cyber ecosystem across Member states and stakeholders</p>
<p>Cybersecurity as an integral part of EU policies: Embedding across all domains of EU policy, avoiding fragmentation and sensitive to sector specifics</p>	<p>Proactive advice and support to EU-level actors through technical guidelines. Cybersecurity risk management frameworks across all sectors</p>
<p>Effective cooperation amongst operational actors within the union in case of massive cyber incidents: Cyber-attacks know no borders and effective cooperation between MSs is needed.</p>	<p>Continuous cross-border and cross layer support to cooperation between MSs as well as with EU institutions. Support scale up of cooperation against potential large-scale incidents. Comprehensive and rapid technical handling upon request of the Member States.</p>
<p>Cutting-edge competences and capabilities in cybersecurity across the union: Building competencies at all levels not only in MS but also in operational communities.</p>	<p>Aligned cybersecurity competencies, professional experience and education structures An elevated base-level of cybersecurity awareness and competences and mainstreaming into new disciplines. Well prepared and tested capabilities to deal with threat level.</p>
<p>High level of trust in secure digital solutions: A common approach and neutral entity is required to strike a balance between societal, market, economic and cybersecurity needs.</p>	<p>Cyber secure digital environment across the EU, where citizens can trust ICT products, services and processes through the deployment of certification schemes in key technological areas.</p>
<p>Foresight on emerging and future cybersecurity challenges: Dialogue to achieve early mitigation strategies to improve EU resilience.</p>	<p>Foresight and future scenarios to understand emerging trends and early assessment of challenges and risks from the adoption of and adaptation to the emerging future options.</p>
<p>Efficient and effective cybersecurity information and knowledge management for Europe: Continuous process of collecting, organising, summarising, analysing, communicating, and maintaining cybersecurity information and knowledge.</p>	<p>Shared information and knowledge management for the EU cybersecurity ecosystem with appropriate methodology, infrastructures and tools</p>

Table 3-1: ENISA 2020 Strategy – Strategic Objectives and Target Achievements

3.2.2 Cybersecurity Research Directions for the EU’s Digital Strategic Autonomy

On April 23, 2021, ENISA published “Cybersecurity Research Directions for the EU’s Digital Strategic Autonomy”⁴⁵, in which the research priorities to support the EU’s digital strategic autonomy are described in terms of current context, challenges and efforts, with a set of recommendations and overall objectives. In addition, the social dimensions, specifically human capacity building and the legal and regulatory frameworks are also highlighted.



The seven prioritised research areas and the top level recommendations provided in this ENISA publication are found in Table 3-2.

Priority Areas	Research	Domain	Objective for the future
Data security		Understanding and mitigating vulnerabilities of AI.	“ Data security needs to go beyond data at rest in the long term , protecting active data in an environment without borders and well-defined lines.”
		Ensuring the availability of machine learning and big data platforms that are sourced, hosted and sustainable in Europe.	
		Developing new technologies for data security and privacy, to support advances in regulations and the emerging needs of the digital society.	
		Explainable AI	
		Securing decision support and actuating	
		Social trustworthiness of AI.	
Trustworthy software platforms		Trustworthy operating systems.	“The long-term objective of trustworthy software platforms is to ensure that deployed software is of sufficient quality and is developed following the ‘secure-by-design’ and ‘secure-by-default’ principles.”
		Trustworthy middleware.	
		Detection of malware and botnets.	
		System and virtualisation security.	
		Secure software development platforms.	
		Risk assessment platforms.	
		Trustworthy sensors.	
Open-cloud software services.			
Cyber threat management and response		Cyber threat intelligence.	“Europe should try to remain autonomous in the long term , as far as cyber threat management and response are concerned.”
		Cybersecurity analytics.	
		Situational awareness.	
		Attack detection, mitigation and response.	
		Deception.	
		Cyber defence.	
		Post-design and post-perimeter defence and response strategies.	
		Trusted information sharing.	

⁴⁵ ENISA Publication « Cybersecurity Research Directions for the EU’s Digital Strategic Autonomy” https://www.enisa.europa.eu/publications/cybersecurity-research-directions-for-the-eu2019s-digital-strategic-autonomy/at_download/fullReport

Priority Areas	Research	Domain	Objective for the future
Trustworthy platforms	hardware	Bootstrap security.	“The long-term objective of trustworthy hardware platforms is to ensure that the EU possesses the capability and capacity to guarantee access and control over high-quality hardware components, in order to meet its industrial development needs as such components become key in almost all products and services that are being developed and commercialised.”
		Hardware-induced vulnerabilities.	
		Side channel attacks.	
		Hardware-anchored cybersecurity tools.	
		Open hardware architecture.	
		Safe sensing.	
Cryptography		Post-quantum cryptography.	“To ensure that the EU retains access to state-of-the-art cryptographic protection , we must invest in the ability to establish, control and verify standards for processes and products that are vital to Europe.”
		Basic cryptographic building blocks.	
		Standards-based maintenance of cryptographic suites.	
		Cryptographic protocols.	
		Tools to support security validation of cryptographic implementations.	
		Strong EU certification authority.	
User-centric security practices and tools		Privacy-enhancing technologies (PET).	“ Developing user-centric security practices and tools will help weave cybersecurity into our digital lives in the longer term... The success of cybersecurity implies long-term sustainable growth of the European digital society.”
		Usable security.	
		Human-centred security and privacy.	
		Security visibility.	
		Social engineering and human errors in cybersecurity.	
		Verifiable computing.	
Digital security	communication	Network services as critical infrastructure.	“The long-term objective of digital communication security is to be able to deploy and operate seamless infrastructure that ensures end-to-end secure communication regardless of whether it relies on virtual means or physical means.”
		Network security.	
		IoT security.	
		Virtual networks.	

Table 3-2: EU Cybersecurity research directions

3.3 European Cyber Security Organisation (ECSO)

In December 2020, ECSO released two documents gathering, respectively, priorities for the definition of a Strategic Research and Innovation Agenda in Cybersecurity and priorities for supporting the implementation of policy, technology, competitiveness and competence-building:

- Input to the Horizon Europe Programme 2021-2027: Priorities for the definition of a Strategic Research and Innovation Agenda in Cybersecurity⁴⁶
- Input to the Digital Europe Programme 2021-2027: Priorities for supporting the implementation of policy, technology, competitiveness, and competence-building⁴⁷

Both documents were intended to be inputs for the Horizon and Digital Europe Programmes 2021-2027.

3.3.1 Input to the Horizon Europe Programme 2021-2027

In this document, ECSO identified four main strategic areas for investment:

- Ecosystem, Social Good & Citizens
- Application Domains & Infrastructure
- Data & Economy
- Basic & Disruptive Technologies

Main strategic areas for investment	Priority areas
Ecosystem, Social Good & Citizens	Approaches, methods, processes to support cybersecurity assessment, evaluation and certification.
	Building and Operating Resilient Systems: Adaptive Software Hardening, Self-Healing systems and RASP.
	Development of digital forensics mechanisms and analytical support
	Cyber ranges and simulation environments.
	Cyber-physical systems security and cyber secure pervasive technology.
Application Domains & Infrastructure	Cyber resilient digitised infrastructures.
	Secure Quantum Infrastructures.
	Cyber secure future communication systems and networks.
	Vertical sectors cyber challenges.
Data & Economy	Data security and malicious use of data.
	End-to-end privacy.
	Economic aspects of cybersecurity.
Basic & Disruptive Technologies	Secure and Trustworthy AIs.
	Software and Hardware cybersecure engineering and assurance.
	Cryptography.
	Blockchains and DLTs.
	IoT Security.
	AI techniques for better security & malicious use of AI.

⁴⁶ Input to the Horizon Europe Programme 2021-2027: Priorities for the definition of a Strategic Research and Innovation Agenda in Cybersecurity: <https://ecs-org.eu/documents/publications/5fdc4c5deb6f9.pdf>

⁴⁷ Input to the Digital Europe Programme 2021-2027: Priorities for supporting the implementation of policy, technology, competitiveness, and competence-building: <https://ecs-org.eu/documents/publications/5fdc4ca16dde0.pdf>

Table 3-3: ECSO Input to the Horizon Europe Programme 2021-2027

3.3.1.1 Ecosystem, Social Good & Citizens

In the area of **Ecosystem, Social Good & Citizens**, five priorities were defined:

1. **Approaches, methods, processes to support cybersecurity assessment, evaluation and certification.** Including security risk assessment schemes, knowledge and tools for cybersecurity culture assessment, multilayer assessment in systems composed by several devices, easy to measure security metrics, specific testing procedures for each assurance level and domain, methods and tools to relate risks and test scenarios, tools and guidelines from a scientific approach, tools and methodologies to address organisational measures (NLP based techniques), tools to continuous evaluation of system behaviour, tools for assessment in specific disruptive technology domains (i.e. AI), combination of security risk assessment with security testing, combination of assessment methods and tools, usage of cyber-ranges to support cyber certification and test schemes, formal verification whenever possible, automation, testing tools as a grey-close-to-black boxes.
2. **Building and Operating Resilient Systems: Adaptive Software Hardening, Self-Healing systems and RASP.** Including adaptive and intelligence application self-protection, AI-based agents for self-healing systems, potential and cost of software hardening, and in the case of embedded systems, run-time on-chip or on-board monitoring techniques for embedded systems, secure-safe and resilient-by design methodology for R&D of future technologies to be deployed into digital products, resilient computer polycentric architectures supported by advanced tools during the design and evaluation phases.
3. **Development of digital forensics mechanisms and analytical support.** Including forensics-related challenges of cloud services ensuring trustworthiness of collected evidence, HPC options for expediting data pre-processing, storage, analysis, correlation, and reporting, AI-based methods complemented by visualisation ones, e.g., ranking and clustering, for supporting forensic investigators, Threat Intelligence, Forensic-by-Design, reliability and security of digital traces, approaches to digital identification, methods of attack attribution, trained personnel and processes, new methodologies and platforms for cooperation among teams and organisations involved in digital forensics, forensic intelligence sharing supported by threat intelligence sharing platforms, privacy-by-design principles in forensic-by-design mechanisms, multi-disciplinary efforts in the technical, legal and ethics domains.
4. **Cyber ranges and simulation environments.** Including methodologies and technologies to cost efficiently create simulation environment of a client infrastructure (like a Digital Twin in manufacturing), Cyber Threat Intelligence (CTI) based threat simulation, virtualisation and contextualisation, specification of an Open API for data interoperability in AI processing of heterogeneous sources of data, cyber ranges allowing easy integration of hardware to allow easy self-virtualization, out of the box software solutions for automated CTI/evidence based background scenario generation with AI support, the aspects of obsolete/legacy software in the infrastructure (especially in the OT environment), an easy to use UI/UX for the software managing the cyber range, AI that supports CTI based scenario, AI for constantly monitoring and setting up simulations of attacks, standardization of key technological aspects of cyber range, cyber ranges for R&D and for testing & certification, cyber ranges for competence building, a common standardised language, creation of "cyber-range content ecosystem", taxonomies/methodologies for cyber ranges, trainings and cyber defence exercises (CDX), an open format for content, exercising and drilling methodologies identifying risk assessment KPIs and supporting simulation solutions, affordable emulations covering industry needs, integration in the digital competence building programmes, integration of simulation-based cyber resilience measurement and competence building into cybersecurity requirements within the Digital Single Market.

5. **Cyber-physical systems security and cyber secure pervasive technology.** Including secure architectures and communications means to build cybersecure CPS from the start, methods for better resilience and security co-design of products and services, including support for safety/security certification from the beginning of the design process, a modelling framework able to capture the properties and dependences of the CPS systems, approaches to capture key security notions to exchange information using the NIST CPS framework language or Meta Attack Language, dynamic, automated and autonomous approaches for prevention, situational awareness, resilience and traceability.

3.3.1.2 Application Domains & Infrastructure

In the area of **Application Domains & Infrastructure**, 4 priorities were identified:

1. **Cyber resilient digitised infrastructures.** Effort should be focused on achieving effective, real-time situational awareness, securing the whole CI lifecycle, addressing the security issues introduced by 5G deployments and other IoT/edge computing architectures, improvement of the identification and reaction to cyber incidents, Increasing trust in the 4th industrial era, Creating an ecosystem of secure, resilient and privacy-friendly Edge infrastructures, Promote European leadership in secure and privacy friendly advanced IoT applications.
2. **Secure Quantum Infrastructures.** Including the analysis of quantum technologies and their impact in classical security mechanisms and vice versa, entailing the study and development of scenario-based risk assessment frameworks and mitigation strategies, Innovations in the area of QKD protocols and Quantum Communications (device independent QKD, satellite quantum communications, continuous variable QKD, system Architectures for Quantum repeaters and secure endpoints, hybrid (classical-quantum) communication architectures, large scale demonstration of QKD infrastructure)
3. **Cyber secure future communication systems and networks.** Including Dynamic and cyber-situational awareness security orchestration of Virtual Network Security Functions (VNSFs), security orchestration in heterogenous and cross-border networks and systems, Optimal allocation of ultra-lightweight virtual security appliances, Evaluation of new security protocols, Leverage of the Authentication, Authorization and Accounting (AAA) and the use of the Extensible Authentication Protocol (EAP) in 4G and the next, 5G, Adaptation or integration of novel protocols in these scenarios through the established protocols and frameworks, Cognitive, autonomic, end-to-end orchestration of future network services, supporting secure, dynamic computing resource pooling and balancing between the edge and the cores, Resource-aware and –efficient security management for applicability at various scales and layers in future networks, Evaluate the security (including risk) at different layers and the dependencies they bring to the deployments, unified certification schemes, Holistic security assurance and management, Risk assessment and security/trust assurance in 5G, Privacy/anonymity preserving frameworks for localization/emergency services, better understanding of cyber threat actors, Security-by-design when developing security and network architecture together.
4. **Vertical sectors cyber challenges.** Including Cyber and physical world convergence, protection and safety to all cyber assets, Interdependencies between critical sectors, Interoperability and information sharing, Cybersecurity approach at supply chain level, Standardisation and strategic autonomy, Circular economy.
 - *Industry 4.0 and ICS:* Vulnerability assessment, penetration testing and certifications (including OT), Connectivity between IoT devices (or rather Industrial IoT) or new software and legacy systems, Secure interaction with the Internet for enabling the B2B data exchange, Distributed Ledger Technology, Human element and other cybersecurity challenges (like edge security, specific ISAC centres for Industry 4.0, IIoT gateway security...).

- *Energy (oil, gas, electricity), and smart grids*: specific processes of Assurance, product life cycle is a key aspect, a well-structured risk assessment and management system, Cyber physical systems (CPS), Cyber secure future communication systems and networks, Cybersecurity solutions, Data protection, IoT security, digital twin cyber range.
- *Transportation (road, rail, air; sea, space)*: Automotive (lightweight authentication and encryption mechanisms to secure V2V and V2I communication, vehicular network segregation techniques compatible with weight and cost constraints, privacy-preserving and scalable cyber-security monitoring techniques, potentially leveraging edge-computing to support anomaly detection and automated reaction to cyberthreats), Rail (risk of attacks associated to the generalization of automation and computerization in the rail vehicles and signalling systems and associated to the use of wireless techniques), Maritime (consider the uniqueness of OT systems ensuring the high reliability and availability of the systems, risks associated to the future Maritime Autonomous Systems), Civil Aviation and UAVS (protecting information flows, protecting navigation and surveillance communications, by-design support to event handling and incident reporting, strengthen command and control links, potentially with redundant communications leveraging a network of ground stations, improving infrastructures, applications of post-quantum crypto in the aviation sector and some other developments specific for Civil Aviation and UAS respectively), Space (new techniques to mitigate risk associated to GNSS, reinforcement of the role of space segments in secure communication (satellites in Quantum Communication Infrastructures for commercial and dual uses), risks associated to the densification of Low Earth Orbit (LEO) SatCom constellations). Together with some other Cross-cutting challenges.
- *Financial Services, e-payments and insurance*: Cybersecurity exercises and awareness, Regulatory Harmonization, Competences and certifications, Specific harmonization on incident reporting, Cybersecurity intelligence sharing.
- *Public services, e-government, digital citizenship*: Privacy and Security by default and design, Interoperability between legacy and new systems, End users trust management, Trusted Identify Exchange, Privacy Enhancing Technologies, DLT and Crypto-currency.
- *Healthcare*: cyber security awareness for healthcare personnel, New methods to prevent and mitigate cyber-attacks, Increased resilience and recoverability of hospital IT infrastructure, physical and cyber security and interdependencies, New tools for identity and access management, Secure deployment and maintenance for dispersed networks of medical objects, Secure system and software development for medical systems and devices, Secure healthcare information sharing, Secure communications with focus on integrity and availability, Secure digitalization of standard medical procedures.
- *Smart cities and smart buildings (convergence of digital services for citizens) and other utilities*: Holistic approaches to smart city protection, Frameworks enabling cities to assess and reduce their overall risk for expected events, and to cope with unexpected events, Solutions for credentials privacy, secure authentication and identity management, Development of blockchain privacy-preserving approaches following a self-sovereign identity management approach, training software engineers and informing users about the security and privacy risks, Privacy Enhancing Technologies, DLT and Crypto Currency, Cyber secure future communication systems and networks (5G/Fog/Edge/Cloud), IoT Security
- *Robotics security*: Risks associated to commercial off- the-shelf (COTS) products, risks associated to insecure communication protocols in Industrial Control Systems (ICS), Network security improvements, edge computing, Mitigation of DDos Attacks, Data protection and compliance, assuring application robustness, secure and trusted interaction between multiple involved parties, secure software engineering tools and principles for secure devices, infrastructures and applications, security debt identification and measurement, procedures to produce concrete security guarantees along the whole product chain, contract-based design to automatically verify security properties in the integration of subsystems, supporting robot's entire lifecycle to achieve a trustworthy robot, CE conformity

assessment, use of AI in robot development life-cycle, distributed and lightweight authorization and authentication mechanisms, development of Intrusion Detection Systems (IDSs) able to cope with multiple devices, networks and platforms, detection of new vulnerabilities linked to the future evolution, interoperability techniques for security and privacy mechanisms, Security audits and certification procedures for production cells and robotic platform, Identification and management of trade-offs and conflicting situations between safety and security aspects, Effective dependability co-engineering mechanisms, Cybersecurity of intelligent swarms and swarm robotics.

- *Agrifood*: employment of Blockchain technologies in the supply chain, issues related to scalability, interoperability, privacy and data governance, increased awareness, trust and uptake of digitisation by smaller farmers, improved technology supporting transparency and accountability through the supply chain.

3.3.1.3 Data & Economy

In the area of **Data & Economy**, 3 priorities were identified:

1. **Data security and malicious use of data.** Including automated ways to test data-driven systems for biased and erroneous results, automated recognition and filtering out of fake/bad data (in particular, training data for AI models), mechanisms to verify data provenance and integrity, models consistent with the observations of experimental data, taking into account data collected by third parties, goals and social acceptability of data processing and Artificial Intelligence algorithms trained without direct access to raw data.
2. **End-to-end privacy.** Including usable mechanisms for citizens, Enable an end-to-end privacy protection, end-to-end encryption, privacy-aware forensic tools, erasure mechanisms, mechanisms for smart devices capable of enabling forensics investigations, solutions for proving data ownership and possession, solid user-defined mechanisms for controlling data access, privacy-preserving real-time data processing mechanisms, PIR systems offering limited information leakage
3. **Economic aspects of cybersecurity.** Including new conceptual approaches to cybersecurity to make the behaviour of all players more incentive compatible and guarantee an optimal level of investment in cybersecurity, exploring the role of cyber insurance and taxation, creation of stronger trust and coordination between public and private players.

3.3.1.4 Basic & Disruptive Technologies

In the area of **Basic & Disruptive Technologies**, 6 priorities were identified:

1. **Secure and Trustworthy AIs.** Including Privacy-aware big data analytics/data mining, Data Trust and Sharing, Protection against internal and external data breaches, Adversarial machine learning, Confidentiality attacks, Model cloning, xAI – Explainable Artificial Intelligence, AI and blockchain, AI and physical attacks, Resilient AI.
2. **Software and Hardware cybersecurity engineering and assurance.** Including Create the technological foundations and IP to design and improve secure systems incorporating trusted components in order to decrease the dependencies in neuralgic points and components and services retrieved from the global market, Creating a pool of trusted IP blocks from open-source pools, Develop tools to design and verify software and trusted electronics, Providing advanced system and board packaging technologies, New techniques, methods and tools to analyse risks, Definition of processes and creation of tools for the overall system security evaluation and certification, Combine blockchain technology with traditional and legacy software, Development of end to end transparent supply chain software solutions supported by blockchain, development of software and firmware ecosystem to enable the transition to a hybrid current architecture.

3. **Cryptography.** Including collaboration to avoid silos and methods and solutions to address the gaps between the theoretical possibilities and the practical implementations of cryptography.
4. **Blockchains and DLTs.** Including Privacy-friendly blockchain systems based on innovative cryptographic schemes, Safer and simpler key management schemes, Strong integration with current and existing trust services, New and innovative consensus algorithms for optimized throughput, Safer and more solid smart contracts languages, Integration with other innovative technologies under the unifying vision of “secure digital transformation”, Interoperability protocols, Support the development of innovative payment systems (including cryptocurrencies) in the context of heavily regulated sectors, Definition of legal frameworks for the adoption of blockchain systems, Support to standardization initiatives, especially EU-based like CEN CENELEC and ETSI.
5. **IoT Security.** Including Challenges at device level, Challenges in connectivity and network layer, Challenges at IoT platform and IoT service layer, Challenges at application layer and related to end-users and Cross-cutting challenges.
6. **AI techniques for better security & malicious use of AI.** Including Machine Learning for cybersecurity, Large-scale, robust threat- and anomaly detection on highly heterogenous and incomplete data to create situational awareness, Predictive security and (semi-)autonomous incident mitigation to support active incident response strategies, protect additional attack surface created by new and emerging technologies for interacting with IT Systems, Understand and anticipate possible malicious use of artificial intelligence.

3.3.2 Input to the Digital Europe Programme 2021-2027

In this document, ECSO defined four main levers that drive the priorities:

- Support to policy implementation
- Support to technology implementation
- Support to competitiveness and market development
- Support to competence building

Main levers driving priorities	Priority areas
Support to policy implementation	Develop tools to support the implementation of EU Cybersecurity Act.
	Threat management and cross-vertical platforms.
	Governance, policy and legal aspects.
Support to technology implementation	Deploying resilient digital infrastructures in the field.
	Platform for privacy management.
	Platform and processes for wide-scale digital identity in Europe:
	Establishing an engineering platform for trustworthy hardware, software and systems.
Support to competitiveness and market development	Investments in Europe and development of regional ecosystems.
	Platforms for market support to SMEs.
	International cooperation and investments.
Support to competence building	Operational, interoperable and cognitive cyber ranges.
	Citizens and social good.
	Jobs and professional skills.

Table 3-4: ECSO's Input to the Digital Europe Programme 2021-2027

3.3.2.1 Support to policy implementation

In the lever of **Support to policy implementation**, three priorities were defined:

1. **Develop tools to support the implementation of EU Cybersecurity Act.** Including Standards and certification for cyber resilient infrastructures – continuous assessment, Vulnerability disclosure and handling processes, develop tools to automate evaluation compliance and checking during the lifecycle.
2. **Threat management and cross-vertical platforms.** Blockchain to improve Information sharing platforms, predictive capabilities for SIEM, Multi-sovereign probes, Response and recovery tools using autonomic principles (self-*), knowledge, training methods and organizational principles, framework for analysis of integrity and correctness of information, new deception schemes and methods for malware intelligence services, A common platform to harmonise approaches and regulatory requirements under the NIS directive.
3. **Governance, policy and legal aspects.** Including collaboration for a regulation/policy framework, mechanisms and methods to identify responsibilities and requirements across the supply chain, security-by-design and data protection by design, legal structures and business rules for data sharing and management in complex, multi-actor and multi-sectoral scenarios (including standardisation efforts), the European Cybersecurity Competence Centre as a platform for international public-private cooperation and information exchange, cybersecurity certification scheme taking into account the "component" and the "process" level, reducing current dependence on other countries' technologies, reducing the fragmentation in transposing EU legislation in MS, ensure a common approach to 5G cybersecurity at EU level, involve MS and industry players to ensure equal development.

3.3.2.2 Support to technology implementation

In the lever of **Support to technology implementation**, four priorities were defined:

1. **Deploying resilient digital infrastructures in the field.** Including new security mechanisms and capabilities to test and analyse security on a realistic scale, new Software Defined Network components, realistic, open-source and configurable tools and simulators to prove new security solutions for 5G, migration strategies for Quantum-Resistant Crypto for larger scale deployments, new methods for modelling technical systems in continuous change, and the development of resilience capabilities in the organizations managing them.
2. **Platform for privacy management.** Including tools for citizens to understand relationship between acceptance of current tracking mechanisms and the importance of provided data, aiming at developing a database of tracking mechanisms.
3. **Platform and processes for wide-scale digital identity in Europe:** decentralised technologies, self-sovereign identity and blockchain. Including new identity management systems, focus on regulatory compliance, universality of access, limited computing resources, adoption of digital identity systems and procedures in specific and at-disadvantage areas and scenarios, support standardization efforts.
4. **Establishing an engineering platform for trustworthy hardware, software. and systems.** Including frameworks that enable assurance and certification based on continuous risk management to standardise a secure development lifecycle, tools to support the entire development lifecycle integrating potentially with other design tools, a technology platform containing of a mix of open and closed source components, reverse engineering capabilities to evaluate ICs with untrusted value chains, define

standards within the EU to understand digital forensics and incident investigation within a common framework, considering technical aspects, legal and human factors.

3.3.2.3 Establishing an engineering platform for trustworthy hardware, software, and systems.

In the lever of **Support to competitiveness and market development**, three priorities were defined:

1. **Investments in Europe and development of regional ecosystems.** A dedicated investment support program (awareness raising activities and community engagement, Cybersecurity Industry Market Radar, Cybersecurity Ecosystems development, Dedicated Matchmaking Platform) and a Pan-European “Cybersecurity Accelerator” as a network of regional ecosystems specialised in cybersecurity (potential services: Local mapping of existing cybersecurity capabilities, Local immersion & regulatory support, Network of sales and resellers at regional level, Business- design service driving development of a shared European roadmap, Investors Roadshow and Investors deck, cascading fund mechanism).
2. **Platforms for market support to SMEs.** An SME Hub as a market support and networking tool for European Cyber SMEs with three main functionalities (the Registry, the “Cybersecurity Made in EU” label and the “European Cyber Quadrants” for the different market sectors).
3. **International cooperation and investments.** Including mapping of the best technologies and services and private investors in cybersecurity, resources for international exchanges available from local agencies with bi-annual or quarterly activities, building a narrative to incentivise foreign companies to access the European market, establishing a permanent forum to allow a close EU-third country cooperation.

3.3.2.4 Support to competence building

In the lever of **Support to competence building**, three priorities were defined:

1. **Operational, interoperable and cognitive cyber ranges.** A "plug n' play" platform to give flexibility on content creation, including different emulation settings (users, attackers, attacks effects...).
2. **Citizens and social good.** Including improving the knowledge and capabilities of citizens and SME's, understanding the evolutions of the social engineering threat landscape, promoting cross-competences collaborations, using simulation, games and virtual/augmented reality, investing in practical trainings and information tools, defining and incorporating competences for the digital age and digital skills, supporting for specialising young people's skills in digital technologies and other areas of economics with regard to their digital transformation, introducing an innovative cybersecurity education system in primary schools.
3. **Jobs and professional skills.** Including supporting projects that perform an aggregation of existing frameworks and controls, pool resources together and develop a European-wide assessment model with a number of skills and sub-skills, an agenda and repository of available resources for “skills DNA”, developing an effective and efficient European professional cybersecurity workforce education and training programme, a competence (job) portal for a clear categorisation of needed competences for a particular job/profile, a specialised Women4Cyber portal.

3.4 Four Pilots: CONCORDIA, CYBERSEC4EUROPE, ECHO, SPARTA

Before the European Cybersecurity Competence Centre in Bucharest becomes operational, the four pilot projects (CONCORDIA, ECHO, CyberSec4Europe and SPARTA) have been established to develop aspects of the Centre and Network. Each pilot has a Roadmap vision, which is briefly described in the following sections.

3.4.1 CONCORDIA

Website: <https://www.concordia-h2020.eu/>

The summary in this section and extracts (as indicated) are based on CONCORDIA's Deliverable **D4.4 "Preliminary Version of D4.4: Cybersecurity Roadmap for Europe by Concordia (M24)"** available on Concordia's website⁴⁸.

CONCORDIA's Roadmap (as at 12.12.2020) covers:

- A threat landscape analysis identified according to five layers of security (device, network, system, data-/application, and user) with additional analysis on the influence of Covid,
- 6 dimensions to address European sovereignty and for which individual Roadmaps (for each dimension) are provided with short- (next two, three years), mid- (around 2025) and long-term (around 2030) timelines
- Other aspects of sustainability and green technology
- A set of Recommendations

CONCORDIA's aim is to take a holistic approach to its Roadmap and as such identifies six dimensions to address European digital sovereignty, as follows:

1. Research and Innovation
2. Education and Skills
3. Economics and Investments
4. Legal and Policy
5. Certification and Standardization
6. Community Building

For each of the above dimensions, a roadmap is provided in the following sections.

3.4.1.1 *Threat Landscape*

CONCORDIA identifies five layers in its analysis of the threat landscape, specifically, device-centric security, network-centric security, system-centric security, data-/application-centric security, and user-centric security, as given in Figure 3-2 (as taken from CONCORDIA Preliminary version of D4.4)⁴⁸.

⁴⁸ CONCORDIA Preliminary version of D4.4 « Preliminary Version of D4.4: Cybersecurity Roadmap for Europe by Concordia (M24):
https://www.concordia-h2020.eu/wp-content/uploads/2021/03/Deliverables_D4.4-M24.pdf

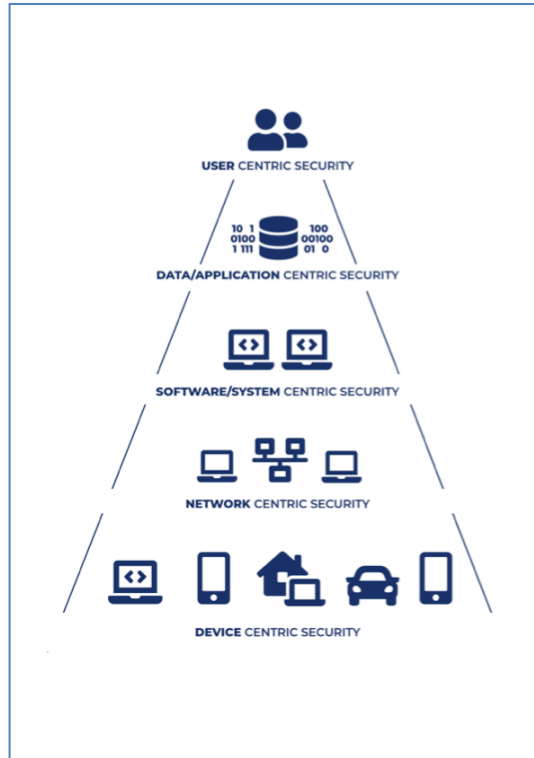


Figure 3-2: CONCORDIA'S Security Layers

CONCORDIA presents its analysis of the threat landscape in Table 3-5 (as taken from CONCORDIA Preliminary version of D4.4⁴⁸), using its threat taxonomy. For each individual threat group the relevant threats in the five layers (domains network, system, device/IoT, data, application and user) are identified.

Domain (D)	Threat Group (TG)	Threats (T)
Device/IoT (1)	Unintentional damage / loss of information or IT assets (1)	Information leakage/sharing due to human errors (1) Inadequate design and planning or incorrect adaptation (2)
	Interception and unauthorised acquisition (2)	Interception of information (1) Unauthorised acquisition of information (2)
	Intentional Physical Damage (3)	Device modification (1) Extraction of private information (2)
	Nefarious activity/abuse (4)	Identity fraud (1) Denial of service (2) Malicious code/software/activity (3) Misuse of assurance tools (4) Failures of business process (5) Code execution and injection (unsecure APIs) (6)

Domain (D)	Threat Group (TG)	Threats (T)
	Legal (5)	Violation of laws or regulations (1)
	Organisational threats (6)	Skill shortage (1)
Network (2)	Unintentional damage / loss of information or IT assets (1)	Erroneous use or administration of devices and systems (1)
	Interception and unauthorised acquisition (2)	Signaling traffic interception (1) Data session hijacking (2) Traffic eavesdropping (3) Traffic redirection (4)
	Nefarious activity/abuse (3)	Exploitation of software bugs (1) Manipulation of hardware and firmware (2) Malicious code/software/activity (3) Remote activities (execution) (4) Malicious code - Signaling amplification attacks (5)
	Organisational (failure malfunction) (4)	Failures of devices or systems (1) Supply chain (2) Software bug (3)
System (3)	Unintentional damage / loss of information or IT assets (1)	Information leakage/sharing due to human errors (1) Inadequate design and planning or incorrect adaptation (2)
	Interception and unauthorized acquisition (2)	Interception of information (1) Unauthorised acquisition of information (data breach) (2)
	Poisoning (3)	Configuration poisoning (1) Business process poisoning (2)
	Nefarious activity/abuse (4)	Identity fraud (1) Denial of service (2) Malicious code/software/activity (3) Generation and use of rogue certificates (4) Misuse of assurance tools (5) Failures of business process (6) Code execution and injection (unsecure APIs) (7)
	Legal (5)	Violation of laws or regulations (1)
	Organisational threats (6)	Skill shortage (1)

Domain (D)	Threat Group (TG)	Threats (T)
		Malicious Insider (2)
Data (4)	Unintentional damage / loss of information or IT assets (1)	Information leakage/sharing due to human errors (1) Inadequate design and planning or incorrect adaptation (2)
	Interception and unauthorized acquisition (2)	Interception of information (1) Unauthorised acquisition of information (data breach) (2)
	Poisoning (3)	Data poisoning (1) Model poisoning (2)
	Nefarious activity/abuse (4)	Identity fraud (1) Denial of service (2) Malicious code/software /activity (3) Generation and use of rogue certificates (4) Misuse of assurance tools (5) Failures of business process (6) Code execution and injection (unsecure APIs) (7)
	Legal (5)	Violation of laws or regulations (1)
	Organisational threats (6)	Skill shortage (1) Malicious insider (2)
Application (5)	Unintentional damage (1)	Security Misconfiguration (1)
	Interception and unauthorized acquisition (2)	Interception of information (1) Sensitive data exposure (2)
	Nefarious activity/abuse (3)	Broken authentication and access control (1) Denial of service (2) Code execution and injection (unsecure APIs) (3) Insufficient logging and monitoring (4) Untrusted composition (5)
	Legal (4)	Violation of laws or regulations (1)
	Organisational threats (5)	Malicious Insider (2)
User (6)	Human Errors (1)	Mishandling of physical assets (1) Misconfiguration of systems (2) Loss of CIA ¹ on data assets (3)

Domain (D)	Threat Group (TG)	Threats (T)
		Legal, reputational, and financial cost (4)
	Privacy breaches (2)	Profiling and discriminatory practices (1) Illegal acquisition of information (2)
	Cybercrime (3)	Organized criminal groups' activity (1) State-sponsored organizations' activity (2) Malicious employees or partners' activity (3)
	Media amplification effects (4)	Misinformation/disinformation campaigns (1) Smearing campaigns/market manipulation (2) Social responsibility/ethics-related incidents (3)
	Organisational threats (5)	Skill shortage/undefined Cybersecurity curricula (1) Business misalignment/shift of priorities (2)

Table 3-5: CONCORDIA Cybersecurity Threat Map

From the analysis of the above threat landscape, CONCORDIA provides a set of technology stack-related recommendations^{Error! Bookmark not defined.}, which are listed in the table below according to the timeframe (short-, mid-, long-term) given in CONCORDIA's Roadmap presented in Figure 3-3.

R#	Recommendations	Short-term	Mid-term	Long-term
R1	Focus on persistent threats	X		
R2	Find a good trade-off between security level and domains peculiarities		X	
R3	Tailored security investments		X	
R4	Protection from insider threats	X		
R5	Consider the deployment environment untrusted		X	
R6	Digital twins and possible safety impact			X
R7	Protect the user profiling capabilities		X	
R8	Protect the AI models, engines, and data pipelines from manipulations		X	
R9	Consider the networking peculiarities while designing system security		X	
R10	Protect from wide-band network-based localized DDoS	X		
R11	Protect edge computing nodes and services		X	
R12	Adoption of serverless computing	X		
R13	Protect against AI weaponized threats		X	
R14	Protection against deepfake			X
R15	Conscious use of Social Networks			X
R16	Deep understanding of layered architecture security	X		
R17	Sharing and multi-tenancy concerns	X		
R18	Consider the Virtualization/Containment weakness	X		
R19	Control misconfiguration issues and foster transparency			X
R20	Avoid shadow IT			X

R#	Recommendations	Short-term	Mid-term	Long-term
R21	Monitoring of human errors	X		
R22	Continuous awareness campaign and training		X	
R23	Protect the CIA triad of data	X		
R24	Protect from mobile and IoT malware	X		
R25	Adopt security-aware development pipelines	X		
R26	Consider the complexity of the deployment environment			X
R27	Consider the miniaturization of the services	X		
R28	Protect CPS devices		X	

Table 3-6: CONCORDIA's Technology stack-related Recommendations

The above recommendations are entered in the context of the Roadmap in Figure 3-3

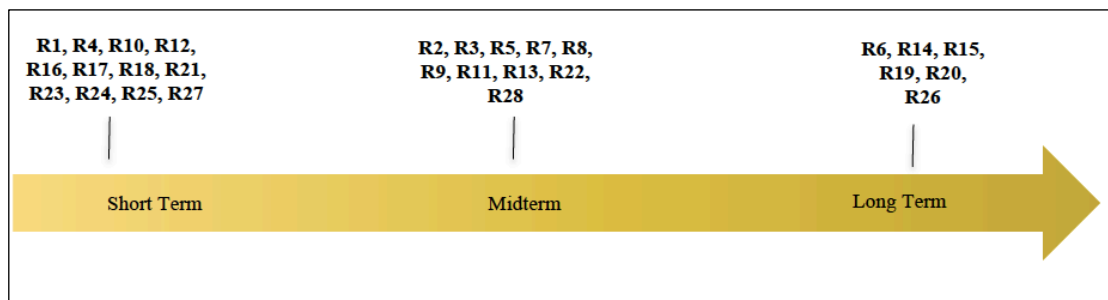


Figure 3-3: CONCORDIA's Overview from technical perspective of most important directions in short-, mid-, and long-term timeframe

3.4.1.2 CONCORDIA's Roadmap for Research and Innovation

CONCORDIA's Roadmap for Research and Innovation addresses the aspect of technological sovereignty, specifically:

- Fighting disinformation
- Data Lakes
- Responsible Internet
- Quantum technologies

Figure 3-4 (from CONCORDIA Preliminary version of D4.4⁴⁸) presents the timeline of most important directions, steps, and threats for short-, mid- and long-term goals.

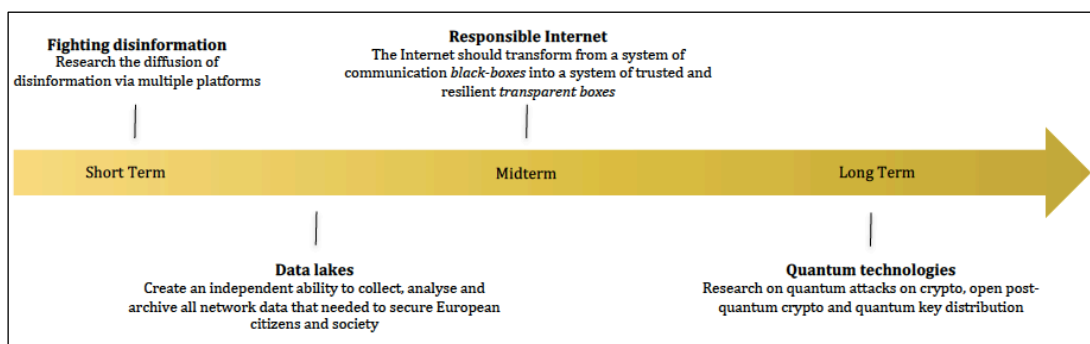


Figure 3-4: CONCORDIA Roadmap for Research and Innovation

3.4.1.3 CONCORDIA's Roadmap for Education and Skills

CONCORDIA Roadmap for Education and Skills examines a list of challenges (C1-C9) and presents their relationship to the related set of recommendations (R1-R13) as illustrated in Figure 3-5 (from CONCORDIA Preliminary version of D4.4⁴⁸).

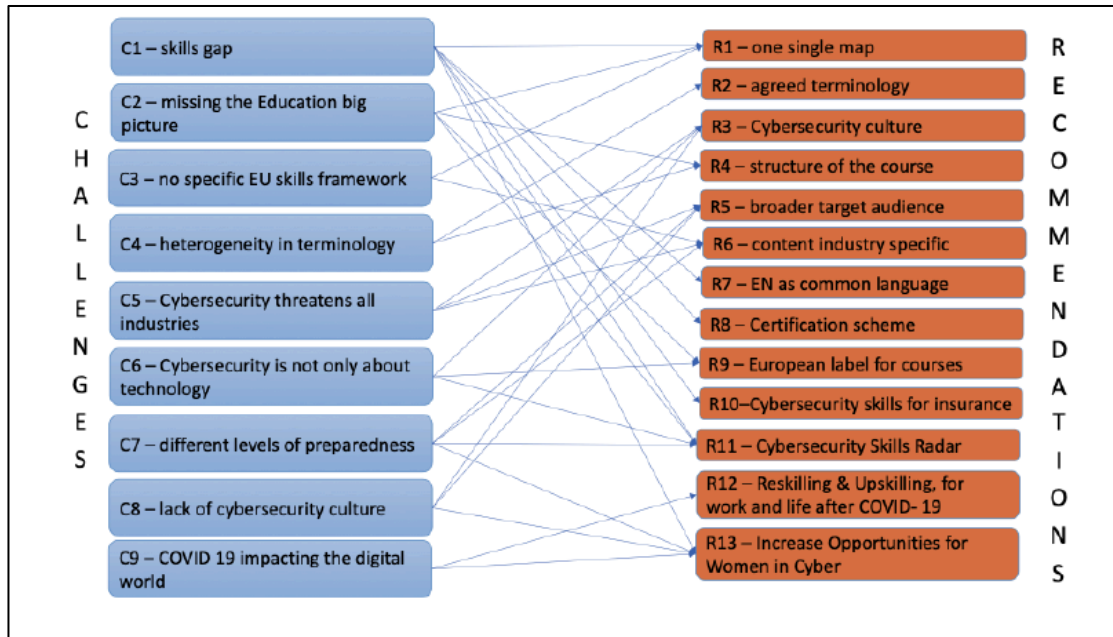


Figure 3-5: CONCORDIA - Relationship between identified challenges & proposed recommendations

The recommendations (R1-R13) are displayed in CONCORDIA’s visual Roadmap in Figure 3-6 (from CONCORDIA Preliminary version of D4.4⁴⁸) which presents the overview from an Education and Skills perspective of the most important directions, steps, and threats for short-, mid-, and long-term timelines linked to Professional Education:

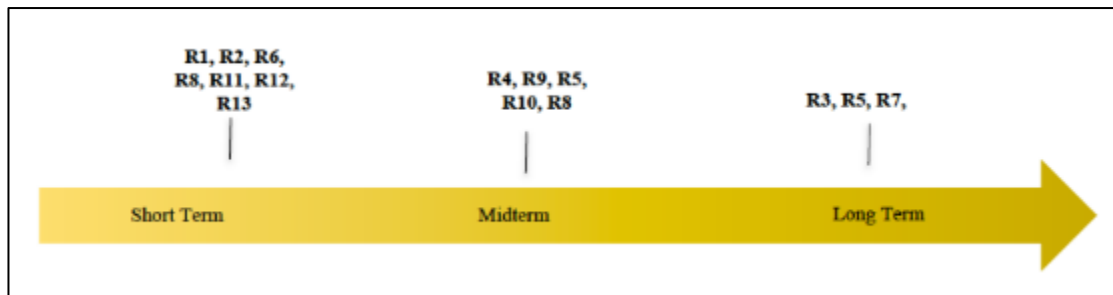


Figure 3-6: CONCORDIA Roadmap for Education and Skills

The summary of the above graphic is given below in Table 3-7.

Recommendation	Short Term	Mid Term	Long Term
R1 - Mapping: one single map	X		
R2 - Terminology: setup and adopt a standard lexicon	X		
R3 – Culture			X
R4 - Structure		X	
R5 – Target			X
R6 – Content	X		
R7 – Language			X
R8 – Certification		X	
R9 - European label		X	
R10 – Insurance		X	
R11 - Cybersecurity Skills preparedness Radar	X		
R12 - Reskilling & Upskilling after COVID-19 pandemic	X		

Recommendation	Short Term	Mid Term	Long Term
R13 - Increase Opportunities for Women in Cyber	X		

Table 3-7: Summary CONCORDIA Roadmap for Education and Skills

3.4.1.4 CONCORDIA’s Roadmap on Economics

CONCORDIA presents its Roadmap on Economics from an Economic perspective of most important directions, steps, and threats for short term, midterm, and long-term timelines, as provided in Figure 3-7: CONCORDIA's Roadmap on Economics (from CONCORDIA Preliminary version of D4.4⁴⁸).

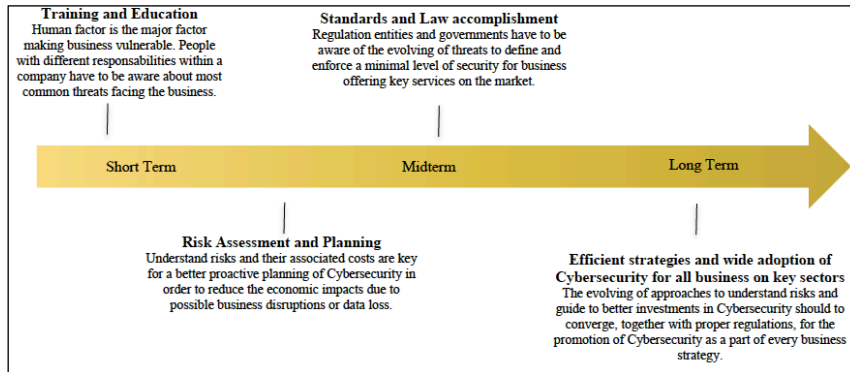


Figure 3-7: CONCORDIA's Roadmap on Economics

The following top-level recommendations are made with further details in CONCORDIA Preliminary version of D4.4⁴⁸:

- R1 - Focus on the risk assessment and planning of cybersecurity
- R2 - Efficient investments on protections
- R3 - Standards and Law accomplishment
- R4 - Cost reduction by using state-of-the-art technologies and Approaches
- R5 - Training and Education
- R6 - Overall Integration of Cybersecurity Economics Modules within EU Cybersecurity

3.4.1.5 CONCORDIA’s Roadmap on Investment

CONCORDIA’s overview from an Investment perspective of the most important directions, steps, and threats for short-, mid-, and long-term timelines is given in Figure 3-8 (from CONCORDIA Preliminary version of D4.4⁴⁸).

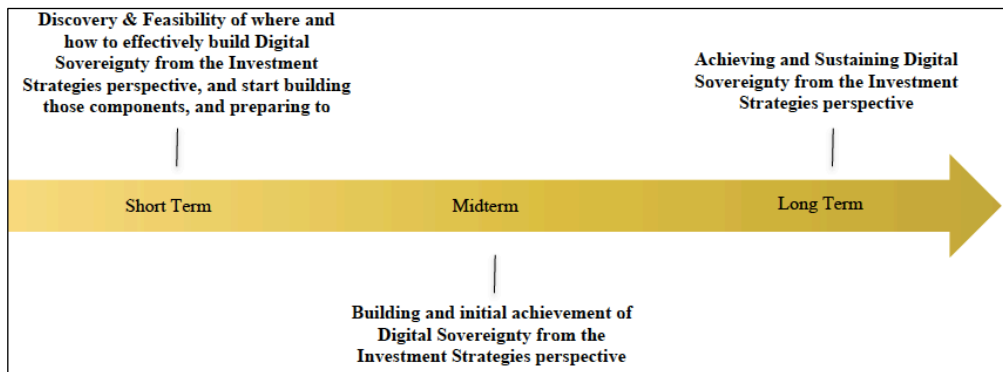


Figure 3-8: CONCORDIA's Roadmap on Investment Strategies

3.4.1.6 CONCORDIA’s Roadmap on Legal and Policy Direction

CONCORDIA’s visual Roadmap from a Legal and Policy perspective of most important directions, steps, and threats for short-, mid-, and long-term timelines is given in Figure 3-9 (from CONCORDIA Preliminary version of D4.4⁴⁸).

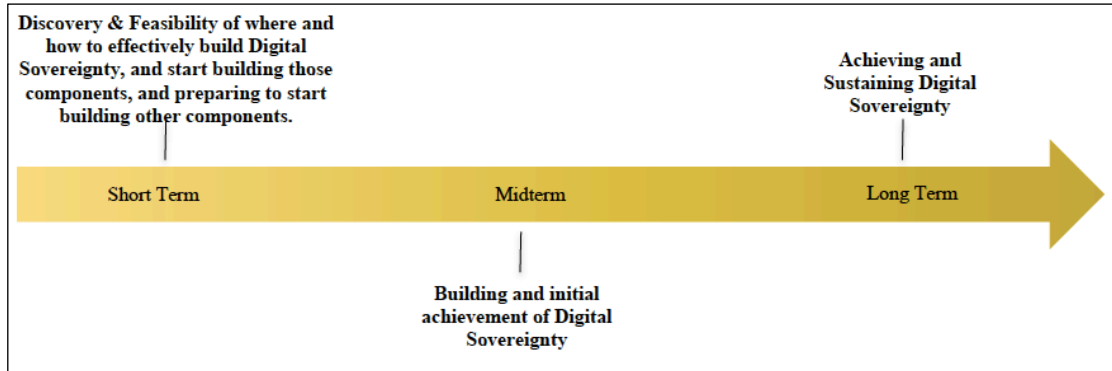


Figure 3-9: CONCORDIA's visualized Roadmap on Legal and Policy

3.4.1.7 CONCORDIA’s Roadmap for Standardization and Certification

CONCORDIA lists the following short-, medium- and long-term aims in standardization as follows in Table 3-8, Table 3-9 and Table 3-10 (from CONCORDIA Preliminary version of D4.4⁴⁸).

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

Table 3-8: CONCORDIA - Short-term standardization aims in standards & certification

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

Table 3-9: CONCORDIA - Mid-term standardization aims in standards & certification

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

Table 3-10: CONCORDIA - Long-term standardization aims in standards & certification^{Error!}

Bookmark not defined.

CONCORDIA lists the following short-, medium- and long-term aims in certification as follows in Table 3-11, Table 3-12 and Table 3-13.

Short-Term Certification Aims	Activity
CA1	Spread the creation of requirements and relevant certification schemes to the different stakeholders, allowing for fast and concurrent development in multiple areas, based on a concrete certification plan
CA2	Create an accepted methodology for testing cybersecurity products and a central certification framework
CA3	Create a European Accreditation framework for the testing and certification of cybersecurity products, processes and systems
CA4	Create a European Accreditation framework for the testing and certification of the privacy of products, processes and systems
CA5	Certification of Product Security Incident Response Team (PSIRT) program for vendors to help their customers in addressing the security of their products in a prompt and efficient way

CA6	Cybersecurity certification scheme for IoT
CA7	Cybersecurity certification scheme for Network devices
CA8	Cybersecurity certification scheme for Cloud services
CA9	Cybersecurity certification scheme for Remote working

Table 3-11: CONCORDIA -Short-term certification aims in standards & certification

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

Table 3-12: CONCORDIA -Mid-term certification aims in standards & certification

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

Table 3-13: CONCORDIA - Long-term certification aims in standards & certification

An Overview from a Certification & Standardisation perspective of the most important directions, steps, and threats for short-, mid-, and long-term timelines is provided by CONCORDIA's D4.4 in Figure 3-10 (from CONCORDIA Preliminary version of D4.4⁴⁸).

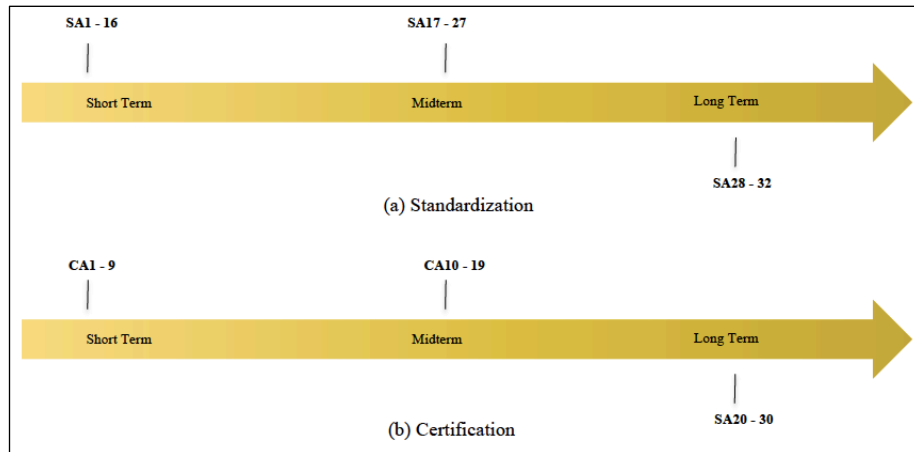


Figure 3-10: CONCORDIA - Standardization & Certification Roadmap

3.4.1.8 CONCORDIA's Roadmap for Community Building

The Roadmap for Community Building will be produced in the next version of CONCORDIA's Cybersecurity Roadmap for Europe. A vision of the different stakeholders and digital ecosystems is available in Figure 3-11 (from CONCORDIA Preliminary version of D4.4⁴⁸).



Figure 3-11: CONCORDIA - Overview of different stakeholders and influencers of digital ecosystems

A view of the short-, mid- and long-term examples of topics to consider in the Roadmap for Community Building (CONCORDIA Preliminary version of D4.4) are provided, as follows:

Short-Term:

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

- Build trust and trustworthiness.

Mid-Term:

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

Long-Term: the focus is to expand, sustain and improve the various living Labs, competence centers and further capability building.

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

3.4.2 Cybersec4Europe

Website: <https://cybersec4europe.eu/>

The CyberSec4Europe project⁴⁹ publishes a yearly research and development roadmap with focus on its research areas of seven verticals. In the lifetime of the project, three roadmaps are foreseen, two of which have been published, as follows:

- The first roadmap (Deliverable D4.3, “Research and Development Roadmap”⁵⁰) was published in 2020 and focused on landscaping the research areas of the verticals and establishing the most important priorities [Markatos 2020].
- The second roadmap (Deliverable D4.4, “Research and Development Roadmap 2”⁵¹ [Markatos 2021]) was published in January 2021. It is intended to be read as a whole roadmap, i.e. it includes information in D4.3, and supplements it with updated research priorities, a SWOT analysis that builds on strengths and shortcomings, and further explains how the research priorities interact with important European dimensions of policies in 2020-2021 with relation to EU digital sovereignty, realities imposed by Covid-19 and the Green deal.

⁴⁹ Pilot Project CyberSec4Europe website: <https://cybersec4europe.eu/>

⁵⁰ CyberSec4Europe Deliverable 4.3 available online at : <https://cybersec4europe.eu/wp-content/uploads/2020/09/D4.3-Roadmap-v5-NEW.pdf>

⁵¹ CyberSec4Europe Deliverable 4.4 available online at: <https://cybersec4europe.eu/wp-content/uploads/2021/02/D4.4-Research-and-Development-Roadmap-2-v3.0-submitted.pdf>

The approach taken is to explore emerging threats and prioritise research directions, mainly in the areas of the **seven verticals** that have been identified by the project, specifically:

1. Open banking,
2. Supply-chain security assurance,
3. Privacy-preserving identity management,
4. Incident reporting,
5. Maritime transport,
6. Medical data exchange,
7. Smart cities.

For each vertical, information is provided on:

- The big picture of that vertical,
- What is at stake, who are the attackers,
- What research challenges are being faced and the final goals,
- What methods and tools are being developed to address challenges,
- Finally, the research challenges that need to be addressed are identified and grouped according to time in three phases: short term (12 months), medium term (until the end of the project), and long term (beyond the end of the project).

3.4.2.1 CyberSec4Europe - Open banking

CyberSec4Europe identifies six challenges in the area of **Open Banking**:

- Challenge 1: Mapping of stakeholder interaction in end-to-end Open Banking processing
- Challenge 2: Setting up and discontinuing business relationships
- Challenge 3: Cross-border cooperation under differing legislation and security controls
- Challenge 4: Convenient and Compliant Authentication
- Challenge 5: Real time Revocation of Right of Access
- Challenge 6: Corporate Open Banking Security

The following is the CyberSec4Europe Summary of their SWOT Analysis for Open banking⁵¹.



Figure 3-12: CyberSec4Europe's - Open Banking SWOT Analysis Summary

The tools required for each challenge and the methods that need to be addressed are given in in Table 3-14. References to Cybersec4Europe Deliverables D3.1⁵², D3.2⁵³.

Open Banking Challenges	Tools/methods required	Tools/methods contemplated for Open Banking	Tools/methods that need to be addressed
Challenge 1	End-to-end processing	Mapping end-to-end processes, taking into account both internal and external systems, involving all stakeholders in B2C banking and payment transactions including users. DP analysers, Security & Privacy by Design (both D3.1, Section 5.1), OFMC/AIF, CORAS (both CyberSec4Europe D3.1, Section 5.2)	Having identified the security and privacy gaps in the end-to-end banking/financial processing chains, a further set of tools will be required to monitor and assess the risk points.
Challenge 2	Severing relationships	A systematic security analysis, modelling and implementation of solutions using modern methods to cover a number of scenarios that are not covered by legislation Trust Monitor (CyberSec4Europe Deliverable D3.1, Section 5.1)	Improved communication between authorities and financial institutions to protect the integrity of the banking/financial ecosystem in case of disruption.
Challenge 3	Harmonisation of national legislation	Policy recommendations on PSD2 to the EC's DG Internal Market	Enhancements on PSD2 legislation to achieve greater harmony on Member State implementation of the directive.
Challenge 3	Harmonisation of access mechanisms	Policy recommendations on harmonising APIs to national/regional open banking organisations, such as OBIE, The Berlin Group et al.	Pan-European agreements to ensure interoperability between the different approaches to open banking access across Europe (and globally)
Challenge 3	Harmonisation of security controls	Policy recommendations to banking associations, starting with the EBA, and participation in standards bodies	A pan-European agreement to ensure that authentication mechanisms across Europe are based on the same levels of security
Challenge 4	Improving the user experience	Recommendation to regulators, and financial community stakeholders to collaborate with user groups and UX designers Mobile pABC (CyberSec4Europe Deliverable D3.1, Section 5.1), HAMSTERS, PetShop (CyberSec4Europe Deliverable D3.1, Section 3.6), Guidelines for GDPR compliant user experience (CyberSec4Europe Deliverable D3.1, Section 3.7)	To simplify the user experience in using open banking user-oriented interfaces and tools without loss of functionality

⁵² CyberSec4Europe D3.1 – Common Framework Handbook #1 <https://cybersec4europe.eu/wp-content/uploads/2020/06/D3.1-Handbook-v2.0-submitted-1.pdf>

⁵³ CyberSec4Europe D3.2 – Cross Sectoral Cybersecurity Building Blocks https://cybersec4europe.eu/wp-content/uploads/2020/06/D3.2-Cross_sectoral_cybersecurity-building-blocks-v2.0.pdf

Open Banking Challenges	Tools/methods required	Tools/methods contemplated for Open Banking	Tools/methods that need to be addressed
Challenge 5	Production of statistics on distributed revocation requests	Data analysis of any encrypted personal banking-related data using homomorphic encryption / secure multiparty computation (SMPC) Sharemind MPC – Privacy-preserving data analysis (CyberSec4Europe Deliverable D3.2 – section 10.2)	Changes to the legislation should be recommended to tighten up the apparent loopholes regarding revocation of consent.
Challenge 6	Mitigation of corporate risks	Similar to Challenge 1, mapping end-to-end processes, taking into account both internal and external systems, involving all stakeholders in B2B banking and payment transactions including corporate users. CORAS, HERMES, OFMC/AIF (all CyberSec4Europe Deliverable D3.1, Section 5.1), Testing, verification and mitigation methodology, SPARTA (both CyberSec4Europe Deliverable D3.1, Section 5.4)	Having identified the security and privacy gaps in the end-to-end B2B transaction processing, a further set of tools will be required to monitor and assess the risk points and take action when vulnerabilities are detected.

Table 3-14: CyberSec4Europe – Challenges and Tools in Open Banking Error! Bookmark not defined.

The timeframe for the Open Banking Vertical (as taken from CyberSec4Europe Deliverable D4.4)⁵¹ is provided in Table 3-15.

Open Banking Vertical - Roadmap Timeframe:
<p>2-year (or until the end of the project) plan:</p> <ul style="list-style-type: none"> By the end of 2022, CyberSec4Europe should have been able to investigate: <ul style="list-style-type: none"> The impact of the discontinuation of relationships in an established trust chain across the various scenarios envisaged in the 12-month plan The technical and non-technical consequences of the mapping exercise in cross-border scenarios, including one-to-one, one-to-many and many-to-many, and beyond that across different jurisdictions based on the challenges outlined in Open banking
<p>Beyond the end of the project:</p> <ul style="list-style-type: none"> There are some further potential security areas to address that perhaps will only be addressed after the end of the project: Improved third party authentication/registration process with Member States’ National Competent Authorities especially in a cross-border context (see recent 1 MEUR open banking fraud between Hungary and the Netherlands) Connectivity of eIDAS certificates (with seals and transport certificates as required by regulation) with emerging PSD2-specific directory services Old “credential sharing” and “screen scraping” technologies (as permitted in PSD2 regulation under certain circumstances) versus modern methodologies (two-factor/SCA) and modern cyber-attacks (especially man-in-the-middle) Role of mobile ecosystem (apps, authentication, biometrics, wireless data, etc.) in PSD2 security Issue of “consent” under GDPR within PSD2: roles/liabilities of actors, conflicts between privacy and payment regulations, need for separate/neutral consent platforms at neither bank nor TPP Risks in the planned next steps in Europe, especially the API “scheme” and new “rich POS solutions” triggering instant credit transfers (with irrevocable fund transfer and limited time to

<p>Open Banking Vertical - Roadmap Timeframe:</p> <p>do full AML/KYC/FATCA/sanction checks) at physical and virtual e-commerce and m-commerce checkouts.</p>

Table 3-15: CyberSec4Europe - Open Banking Timeframe

3.4.2.2 CyberSec4Europe Vertical – Supply Chain

CyberSec4Europe identifies four challenges identified in the area of **Supply Chain**, as follows:

- Challenge 1: Detection and management of supply chain security risks
- Challenge 2: Security hardening of supply chain infrastructures, including cyber and physical systems
- Challenge 3: Security and privacy of supply chain information assets and goods
- Challenge 4: Management of the certification of supply partners

The following is the CyberSec4Europe Summary of their SWOT Analysis for Supply Chain vertical (as taken from CyberSec4Europe Deliverable D4.4⁵¹).



Figure 3-13: CyberSec4Europe - Supply Chain - SWOT Analysis Summary

The tools required for each challenge and the methods that need to be addressed are given in Table 3-16⁵¹.

Challenge	Tools required for	Tools contemplated for Supply Chain	Tools/Methods that need to be addressed
Challenge 1	Risk management methodologies	Guidelines for GDPR compliant user experience (CyberSec4Europe Deliverable D3.1, Section 5), and general-purpose methodologies such as CORAS (CyberSec4Europe Deliverable D3.1, Section 5.2)	Adaptation of recognized SCRM methodologies, lightweight and automated mechanisms for supply chain scenarios
Challenge 2	Detection, Continuous monitoring and incident management	Briareos (CyberSec4Europe Deliverable D3.1, Section 5.3) and NextGen	Behavioural-based approaches and consensus-based algorithms, and proactive detection through

Challenge	Tools required for	Tools contemplated for Supply Chain	Tools/Methods that need to be addressed
		(CyberSec4Europe Deliverable D3.1, Section 5.3)	machine-learning or data-mining. Lightweight SIEMs with ability to contemplate the specific complexities of the context
Challenge 3	Traceability	Self-sovereign identity management (CyberSec4Europe Deliverable D3.1, Section 5.1), Cryptovault (CyberSec4Europe Deliverable D3.1, Section 5.1)	Digital profile for actors/assets, blockchain-based smart contracts and events, automatic analysis mechanisms
Challenge 3	Shared data spaces	Privacy-preserving middleware (CyberSec4Europe Deliverable D3.1, Section 5.6), PLEAK (D3.1, Section 5.6)	Secure shared data space infrastructure with access control and data policies
Challenge 4	Continuous certification	Briareos (CyberSec4Europe Deliverable D3.1, Section 5.3)	Penetration testing, security analysis tools, threat intelligence

Table 3-16: CyberSec4Europe - Challenges and Tools in Supply Chain

The timeframe for the Supply Chain Vertical (as taken from CyberSec4Europe Deliverable D4.4)⁵¹ is provided in Table 3-17.

Supply Chain Vertical - Roadmap Timeframe:
<p>12-month plan: For the next 12 months, CyberSec4Europe will focus on the following aspects of supply chain security:</p> <ul style="list-style-type: none"> At present, there are already various tools and mechanisms that can provide penetration testing and software analysis services for supply chain ecosystems. For the protection of IT/OT infrastructures and networks and the compliance with regulations, it is necessary to <i>apply such tools to test not only the supply chain infrastructure but also the supply chain goods—both software and hardware (firmware)</i>. More specifically, the existence of novel certifications and guidelines in this regard will push the integration of such mechanisms into existing supply chain processes over the next year. Blockchain is already being used to exchange information related to supply chain events. Thus, the plan for blockchain-based solutions in the next 12 months is focused on the <i>integration of distributed workflow operations management</i> in supply chains through smart contracts, as there are already blockchain solutions that provide support for the exchange of basic information through blockchains. Therefore, it is now possible to explore the usage of tokens for representing information about a workflow, such as starting business processes only when all necessary tokens are available. The integration of such processes can also facilitate the applicability of accountability processes in case of conflict.
<p>2-year (or until the end of the project) plan For the next 2 years, we need to focus on the following aspects of supply chain security:</p> <ul style="list-style-type: none"> Regarding the protection of IT/OT infrastructure of supply chains, there are various aspects that can be made available and/or improved in two years' time. As for the trusted exchange of information, it is necessary to advance more in the area of <i>sharing information about software assets</i>, which will provide a foundation for the security of the software supply chain. There is also ongoing work and research on applications that facilitate the automation of certain aspects of supply chain risk management programs. These include, among others, the <i>specification and analysis of cyber kill chains</i> that will highlight the weakest points in the supply chain ecosystem, and the definition of <i>continuous vulnerability analysis</i>

Supply Chain Vertical - Roadmap Timeframe:

processes that monitor the compliance of certain supply chain processes. It is to be expected that these aspects will be refined in two years' time.

- As for the 2-year plan and the integration of **blockchain-based solutions**, there are various avenues that can be explored in this period of time. One such avenue is the *integration of accountability protocols* that could be used in case of conflict, where trusted third parties can manually review the workflow and resolve conflicts if it is apparent that an entity has not behaved according to the established rules. Another avenue is related to *exploring the integration of GDPR enforcement solutions*, where processes and workflows implemented in the blockchain can comply with existing regulations. Other aspects include *self-sovereign identity solutions*, and *the exchange of private data through various means*.

Beyond the end of the project plan:

Regarding blockchain-based solutions, **future solutions could take full advantage of the properties of the blockchain** to fulfil its goal as a mechanism that can be used to protect the security and privacy of all assets and goods. The mechanisms that are needed to fulfil this goal include the *exchange of data between different blockchains*, the *execution of automated tasks* (outside or inside various blockchains) *to automatically monitor the state of a complex interconnected supply chain*, a *deeper integration with existing frameworks, such as compliance requirements and clearance processes*, and *the implementation of self-sovereign identity approaches to manage certain actors and assets of supply chains*.

Another avenue of research is related to the supply chain risk management and compliance with regulations, where **the integration of automatic mechanisms that can continuously analyse and pinpoint potential and/or existing security and privacy issues in all assets** can be used for several purposes, including: i) the *integration of continuous certification processes* that can attest the security of supply chain infrastructure, hardware assets and goods, and software assets and goods; and ii) the *implementation of better supply chain risk management policies* that consider not only a failure in Tier 1 partners but also potential cascade effect issues.

Another aspect to take into consideration is **the availability of autonomous self-healing processes**, which will facilitate the automatic recovery and reconfiguration of states, processes or parameters in IT-OT networks - an essential aspect to guarantee at all times business continuity in (hyper-)connected supply chain networks. One technology that can facilitate this are the **"smart" (and distributed) digital twins**, which could make possible both the prediction and reconfiguration of the system. Still, there are various research challenges associated with this concept, including: *how to manage the "trust" in the two-way interface between the real and physical world*, and *how to integrate digital twins as part of the IT-OT infrastructure* (including technologies such as cloud and IoT) *in a secure way*.

Finally, the advent of **Artificial Intelligence and Big Data applied to security and privacy of IT-OT infrastructures**, plus other tools such as **threat intelligence sharing**, can provide multiple benefits to supply chain infrastructures, including: i) *optimizing and improving the decision-making processes and response for cyber intelligence*, so as to achieve a better awareness of the situation, and achieve a better governance of the system; and ii) *automatically harden supply chain IT-OT infrastructures* due to the better knowledge of the infrastructure and its risks.

Table 3-17: CyberSec4Europe - Supply Chain Vertical Timeframe

3.4.2.3 CyberSec4Europe Vertical - Privacy-Preserving Identity Management

CyberSec4Europe identifies seven challenges identified in the area of **Privacy-Preserving Identity Management**, as follows:

- Challenge 1: System-based credential hardening
- Challenge 2: Unlinkability and minimal disclosure
- Challenge 3: Distributed oblivious identity management
- Challenge 4: Privacy preservation in blockchain
- Challenge 5: Password-less authentication
- Challenge 6: GDPR and eIDAS impact on Identity Management

Challenge 7: Identity Management Solutions for the IoT

The following Figure is the CyberSec4Europe Summary of their SWOT Analysis for the Privacy-Preserving Identity Management vertical⁵¹.



108

Figure 3-14: CyberSec4Europe - Privacy-Preserving Identity Management SWOT Analysis Summary

The tools required for each challenge and the methods that need to be addressed are given in Table 3-18 (as taken from CyberSec4Europe Deliverable D4.4⁵¹).

Challenge	Tools required for	Tools contemplated for Privacy-Preserving Identity Management	Tools/Methods that need to be addressed
Challenge 1	System-based credential hardening	modssl-hmac (CyberSec4Europe Deliverable D3.1 Section 5.2)	Making leakage passwords cracking hard
Challenge 2	Unlinkability and minimal disclosure	Mobile pABC, eABCs, ArchiStar (CyberSec4Europe Deliverable D3.1, Section 5.1)	Attribute-based credentials privacy methods and technologies
Challenge 3	Distributed Oblivious identity management	Self-sovereign identity management, Privacy Preserving Middleware, Argus, Cryptovault, Scalable and Private Permissioned Blockchain (CyberSec4Europe Deliverable D3.1, Section 5.1)	Distributed systems for oblivious identity
Challenge 4	Privacy preservation in blockchain	Self-sovereign identity management (CyberSec4Europe Deliverable D3.1, Section 5.1),	Application of privacy methods to blockchain
Challenge 5	Password-less authentication	Password-less authentication (CyberSec4Europe Deliverable D3.1, Section 5.1)	Alternative authentication methods
Challenge 6	GDPR guidelines and eIDAS interoperability	Guidelines for GDPR-compliant user experience and analysis of interoperability and cross-border compliance issues (CyberSec4Europe Deliverable D3.1, Section 5.7).	Comprehensive guideline on applying GDRP and current eIDAS interoperability issues

Challenge	Tools required for	Tools contemplated for Privacy-Preserving Identity Management	Tools/Methods that need to be addressed
Challenge 7	Identity Management Solutions for the IoT	eABCs	

Table 3-18: CyberSec4Europe - Challenges and Tools in Privacy-Preserving Identity Management²⁴

The timeframe for the Privacy-Preserving Identity Management Vertical (as taken from CyberSec4Europe Deliverable D4.4)⁵¹ is provided in Table 3-19.

Privacy-Preserving Identity Management Vertical - Roadmap Timeframe:
<p>For the next 12 months, CyberSec4Europe will focus on the following aspects of Privacy-Preserving Identity Management:</p> <p>Unlinkability and minimal disclosure. Improve the p-ABC system that has been proposed to fulfil the unlinkability and minimal disclosure requirements (included in the distributed oblivious identity management system) with range proofs (allowing complex numerical predicates), and other general improvements that increase the maturity of the implementation.</p> <p>Distributed oblivious identity management. Continue consolidating the distributed oblivious identity management system based on the needs detected in current implementation efforts. For instance, we plan to improve the interoperability of the solution by integrating the p-ABCs with the W3C emerging standards (Verifiable Credentials and Presentations).</p> <p>Privacy preservation in blockchain. Start the integration of the privacy preserving technologies (specifically, the system devised for distributed oblivious identity management) with blockchain to the point of acquiring a mature implementation that allows demonstration of the main functionality through proof of concept deployments.</p> <p>Password-less authentication. For the deployment of the password-less authentication solution we are planning to implement a biometric authentication method that relies on the FIDO protocols and is device-centric. The previous year, the authentication system’s requirements were thoroughly studied, and the system’s architecture was designed. Later, a comparison was performed between the different FIDO versions to find the most appropriate based on the current requirements. We concluded that two FIDO versions will be implemented: FIDO UAF and FIDO 2, to expand the system’s capabilities to support web authentication. The plan for 2021 is to finish the development of the password-less authentication system, namely the development of the client and server applications that will constitute the authentication system.</p>
<p>2-year (or until the end of the project) plan:</p> <p>For the next 2 years, CyberSec4Europe will focus on the following aspects of Privacy-Preserving Identity Management:</p> <p>Distributed oblivious identity management. The final goal for the 2-plan year is the deployment of a distributed oblivious identity management system that fulfils the security and privacy requirements. In this plan, several activities are contemplated. We will continue with tasks involving the design of the system architecture, development of cryptographic components and framework integration. The development of these tasks will be iterative, pilots for the use cases will be deployed and used to evaluate user experience and compliance with legal requirements.</p> <p>Unlinkability and minimum disclosure. As a short- to medium-term research initiative, the analysis of several additional functionalities for anonymous credential systems is envisioned. For instance, we plan to design issuer-hiding ABC system, which only prove that one possesses a credential from one of a set of issuers. Such systems would allow one to prove, e.g., that one possesses a university degree without revealing the issuing institution, thereby directly overcoming challenges of the respective demonstrator case. Another envisioned extension is the combination of ABC systems with state-of-the-art access control mechanisms. This would reduce the number of necessary authentication steps of the end user, as she could reveal all information a</p>

Privacy-Preserving Identity Management Vertical - Roadmap Timeframe:

certain institution (e.g., hospital) might require, while still having formal guarantees that each employee would only be able to access the required amount of information (e.g., doctors would be able to access other parts of the same presentation token than the hospital administration or the patient's insurance company). Reference implementations to demonstrate the efficiency and scalability of these extensions are foreseen.

Privacy preservation in blockchain. For the remaining two years of the project, the plan can be divided in two phases. The first comprises the next 12 months and it is detailed in the previous section. For the last 12 months, we should part from a *mature implementation* with demonstrable core functionalities. Finally, during the third year, the **full integration** should be completed **to accommodate a set of well-defined use cases**, permitting testing and measurement processes that will check and verify the performance and usability of the proposed solution.

Password-less authentication. By the end of 2022 we are planning to perform a pilot usage of the system to improve the user experience process, since usability is regarded as one of the most important attributes of an authentication system. In parallel with the pilot usage, we will focus more on the system's privacy. Particularly, we will integrate an ABC solution to our password-less authentication system to offer privacy-preserving capabilities. From 2023 and beyond, we intend to update the system's features in order to improve its usability by implementing more authenticators (e.g., voice recognition) and meet the needs that will have been arisen at that period.

System-based credential hardening. To address system-based credential hardening, we plan to **incorporate cryptographic services for hardening text-based passwords in the prototype of the distributed oblivious identity management system**. Additionally, we plan to carry out research for **incorporating credential hardening for non-textual credentials**.

GDPR guidelines and eIDAS interoperability. Iterative analysis of interoperability and cross-border compliance of the eIDAS compliant electronic identification, security, and authentication services will be performed to identify flaws and compatibility of solutions between member states

Beyond the end of the project plan:

The following research challenges will be worked on by CyberSec4Europe partners only after the project duration:

GDPR guidelines and eIDAS interoperability. We have mentioned, the GDPR is a very loose set of rules, often dependent on how the European Court of Justice, the supervisory authorities and often big players in the industry interpret the regulation. All of this is also subject to change over time. This could make the guidelines provided in the project become obsolete. Issues and other findings with the eIDAS interoperability will also change through time. That is why continuous support, even beyond the scope of the project, is necessary.

Identity Management Solutions for the IoT. While the related research activities within CyberSec4Europe have finished after the feasibility result in [HK 2019] by designing a cloud-based privacy-preserving authentication mechanism, mid-term plans include the design of lightweight protocols built (mainly or exclusively) from symmetric primitives, an approach that has been followed, e.g., for group signatures by Boneh et al [BEF19].

Post-Quantum Scenario. Recent advances in quantum computing threaten the security of the current IoT using traditional cryptographic schemes. We are at the very beginning of the standardization process for quantum resistant algorithms, and research on their application in the IoT is limited. Anticipating the post-quantum scenario in addition to reducing computational requirements may also directly give rise to resistant authentication algorithms in this type of scenarios.

Table 3-19: CyberSec4Europe Privacy-Preserving Identity Management Timeframe

3.4.2.4 CyberSec4Europe Vertical -Incident Reporting

CyberSec4Europe identifies three challenges identified in the area of Incident Reporting, as follows:

- Challenge 1: Lack of harmonization of procedures
- Challenge 2: Facilitate the collection and reporting of incident and/or data leaks
- Challenge 3: Promote a collaborative approach for sharing incident reports to increase risk quantification, mitigation and thus overall cyber resilience

The following Figure is the CyberSec4Europe Summary of their SWOT Analysis for the Incident Reporting vertical (as taken from CyberSec4Europe Deliverable D4.4⁵¹).



Figure 3-15: CyberSec4Europe – Incident Reporting SWOT Analysis Summary

The tools required for each challenge and the methods that need to be addressed are given in Table 3-20 (as taken from CyberSec4Europe Deliverable D4.4⁵¹).

Challenge	Tools required for	Tools contemplated for Incident Reporting	Tools/Methods that need to be addressed
Challenge 1	Incident management, workflow enforcement and event classification.	AIRE - Atos Incident Reporting Engine (CyberSec4Europe Deliverable D3.1, Section 5.4)	Design of data model for data collection of information required for mandatory incident reporting in the financial sector and development of an Incident Register database. Design and implementation of workflow for mandatory incident reporting in the financial sector. Adaptation/extension of the open source incident management tool TheHive to support mandatory incident reporting workflow in financial sector and event classification.

Challenge	Tools required for	Tools contemplated for Incident Reporting	Tools/Methods that need to be addressed
Challenge 2	Data collection, incident management and reporting	AIRE - Atos Incident Reporting Engine (CyberSec4Europe Deliverable D3.1, Section 5.4) and HADES – Automatic analysis of malware samples (D3.1, Section 5.3)	Adaptation of the open source incident management tool TheHive and integration with HADES and AIRE for data collection and mandatory incident reporting workflow enforcement. Generation of reports based on information collected according to the different regulations in the financial sector.
Challenge 3	Threat intelligence data sharing	TATIS - Trustworthy APIs for enhanced threat intelligence sharing, Reliable-CTIs - Reliable Cyber-Threat intelligence sharing, TIE - Threat Intelligence Integrator (CyberSec4Europe Deliverable D3.1, Section 5.3)	Mechanisms to improve trustworthiness and reliability for threat intelligence data sharing using MISP and qualification of IoCs to improve actionability.

Table 3-20: CyberSec4Europe - Challenges and Tools in Incident Reporting

The timeframe for the Incident Reporting vertical (as taken from CyberSec4Europe Deliverable D4.4)⁵¹ is provided in Table 3-21:

Incident Reporting Vertical - Roadmap Timeframe:
<p>12-month plan:</p> <p>During the first part of the project, we have focused on Challenges 1 and 2, aiming to provide a prototype for an incident reporting platform that helps the incident reporting teams of financial institutions to fulfil the requirements of mandatory incident reporting to the Supervisory Authorities, in particular under the PSD2 and ECB regulatory frameworks.</p> <p>We have extended the functionalities of TheHive, an open source incident management tool, to support a workflow for mandatory incident reporting in the financial sector under different applicable regulations (using CS4EU²³³ WP3 assets and specific configuration and templates).</p> <p>During the next 12 months, we plan to start working on Challenge 3, integrating the incident reporting platform through MISP with a threat intelligence sharing platform. Information registered in the incident reporting database will be analysed and shared, and mechanisms will be applied to improve trustworthiness and reliability. Research will be also carried out into the integration of assets in the platform for the qualification of threat intelligence data and the quantification of risks.</p> <p>Related to Challenges 1 and 2, the plan for next year is to improve the current incident reporting platform prototype by including requirements defined in D5.1 but not yet covered, and the generation of interim and final reports for the currently supported regulatory frameworks PSD2 and ECB. This means that the data collection will need also to be extended to include the additional information required for those reports. We will also try to extend the regulatory frameworks supported.</p>
<p>3-year (or until the end of the project) plan:</p>

Incident Reporting Vertical - Roadmap Timeframe:

The plan until the end of the project is to continue consolidating and improving the incident reporting platform regarding these two points:

- extending the number of regulatory frameworks applicable to the financial institutions supported by the platform. In particular, our goal is to include by the end of the project:
 - Personal Data Breach notification under GDPR.
 - Incident Reporting for Operators of Essential Service under the NIS Directive.
 - Incident Reporting for Target2 participants.
 - Incident Reporting for Trust Service Providers under the eIDAS regulation.
- Integration in a trustworthy and reliable way with a threat intelligence sharing platform.

Beyond the end of the project plan:

Digitalization and an increased connectivity play a pervasive role in society and have become the backbone of the growth of economic sectors, thus increasing cybersecurity risks and making society as a whole more vulnerable to cyber threats. While this demonstrator will only cover the Mandatory Incident Reporting requirements for the financial sector as defined by European regulators, the scope of the need it addresses can be extended to tackle similar challenges across different industries, all of which have the common aim of enhancing the cyber resilience of the Digital Single Market and promoting information sharing across multiple industries and public interest sectors.

The first challenge this demonstrator will address after the lifetime of the project is the extension of its scope of applicability from the mandatory to the voluntary sharing of information on cyber vulnerabilities and threats. Far from being an exclusively technical challenge, notable effort will have to be devoted to building the necessary trust among the entities taking part in the information sharing network.

The second challenge and great opportunity is to deploy such an approach across industries, including both private and public players. This could involve not only the financial sector, but also other sectors that face similar cybersecurity challenges and that could benefit from the knowledge acquired through the experience and the best practices of its users. Indeed, looking at the NIS Directive, finance is only one of several critical sectors that are deemed fundamental for the good function of the Digital Single Market and are recognized as being essential to economic and societal activities.

A third opportunity is to look at widening the geographical scope of the platform, taking into account the jurisdictions beyond the EU borders. While the initial perimeter will be limited to the EU Member States, a further extension to the strategic partners of the EU could also be envisaged.

Additionally, an interesting opportunity is to look into innovative technological solutions to be leveraged in the implementation of the smart incident reporting platform. Since a significant part of the demonstrator's challenge consists in being able to devise secure channels of communication among trusted entities willing to share potentially sensible information, an option could be to appropriately leverage the blockchain technology.

Finally, depending on the outcome of the above-mentioned challenges and on the future developments of EU's cybersecurity regulatory framework, the incident reporting platform could become a valuable data source and may contribute consistently to the general enhancement of the cyber resilience of the Digital Single Market. The information collected through the platform could be especially relevant for the future further development and improvement of the following aspects:

- **Assessment and redress of regulatory gaps and incoherencies.** The existing fragmented implementation of policies and uneven transposition of EU regulations among EU Member States result in legal and operational incoherencies that could threaten the achievement of the overall regulatory objectives. In addition, new gaps and incoherencies will keep emerging as the cybersecurity landscape evolves. In this context, the information collected by the incident report platform could be used to support future relevant developments of the

Incident Reporting Vertical - Roadmap Timeframe:
<p>cybersecurity regulatory framework itself. Beyond the lifetime of the project, the platform could (a) provide crucial information for the identification of existing and future gaps and incoherencies; (b) enable the development of the appropriate regulation alternatives and adjustments.</p> <ul style="list-style-type: none"> • Assessment of the achievement of policy objectives and development of evidence-based policy. The information collected by the incident reporting platform could also address the current lack of official data collection on cyber-related matters by EU Member States and enable the future development of evidence-based EU cybersecurity policy. Both the development of evidence-based cybersecurity policies and the assessment of the achievement of the policy's proposed objectives depend on the availability of reliable data and on the definition of appropriate assessment criteria that could arise from the use of the incident report platform. • Assessment and quantification of Operational Risks. As a further refinement of the development of evidence-based policy the ability to provide quantification of risks based on incidents and by using qualifying indicators to estimate the actual impact on one's own infrastructure (see Challenge 3) would bring as a benefit a quantification of a risk area that has been so far mostly qualitative and that could bring significant saving in terms of more precise and optimal assessment and investment in resources. This possibility would strengthen both the individual stakeholders and the overall regulatory regime. • Development of law-making and implementing processes. Furthermore, the data collected by the incident reporting platform could also assist EU legislators to address the current need for innovative and more flexible procedures regarding the development and the implementation of EU legislation in general, and especially of technology-related regulations. The exponential speed of the development of technologies has already outpaced the EU's ability to design and implement regulations, creating a gap that must be addressed by EU legislators in the near future. In this context, the data collected by the incident report platform could guide the development of new EU law-making and implementing procedures, aiming to guarantee that such procedures are flexible enough to ensure a fit for purpose policy and legislative framework.

Table 3-21: CyberSec4Europe Incident Reporting Timeframe

3.4.2.5 CyberSec4Europe Vertical -Maritime Transport

CyberSec4Europe identifies five challenges in the area of **Maritime Transport**, as follows:

Challenge 1: Early identification and assessment of risks, threats and attack paths for critical maritime systems

Challenge 2: Security hardening of maritime infrastructures, including cyber and physical systems

Challenge 3: Resilience of critical maritime systems

Challenge 4: Maritime system communication security

Challenge 5: Securing autonomous ships

The following Figure is the CyberSec4Europe Summary of their SWOT Analysis for the **Maritime Transport** vertical (as taken from CyberSec4Europe Deliverable D4.4⁵¹):



Figure 3-16: CyberSec4Europe – Maritime Transport SWOT Analysis Summary

The tools required for each challenge and the methods that need to be addressed are given below (as taken from CyberSec4Europe Deliverable D4.4⁵¹).

Challenge	Tools required for	Tools contemplated for Maritime Transport	Tools/Methods that need to be addressed
Challenge 1	Early identification and assessment of risks, threats and attack paths for critical maritime systems	Collaborative Risk Management methodologies and risk assessment tools, such as MITIGATE (CyberSec4Europe Deliverable D3.1, Section 5.4), CORAS (CyberSec4Europe Deliverable D3.1, Section 5.2) and BowTie Plus (CyberSec4Europe Deliverable D3.1, Section 5.2)	Utilisation of effective, collaborative, standards-based, risk management methodologies and model-driven approaches to address sector-specific security requirements (Capturing risks and threats arising from the global maritime supply chain, including those associated with the port's CII interdependencies and those related to cascading effects). Development of stable data sets for the maritime environment. Adaptation of efficient cyber-attack path discovery algorithms using predictive analytics and simulation techniques to capture the interdependencies among maritime interconnected systems and support the generation of alternative attack paths, as well as their assessment in terms of risk.

Challenge	Tools required for	Tools contemplated for Maritime Transport	Tools/Methods that need to be addressed
Challenge 2	Security hardening of maritime infrastructures, including cyber and physical systems	TypeArmor (CyberSec4Europe Deliverable D5.2, Section 6.2) and VTPin (CyberSec4Europe Deliverable D5.2, Section 6.2)	Software analysis and identification of unsafe components. Provide security controls at the compiler level, and runtime security mitigations. Utilize binary-level analysis techniques and methodologies for program hardening with no recompilation. In addition, entirely program-agnostic techniques that are will be explored, such as pre-loading the binary with secure memory.
Challenge 3	Resilience of critical maritime systems	MITIGATE (CyberSec4Europe Deliverable D3.1, Section 5.4), CORAS (CyberSec4Europe Deliverable D3.1, Section 5.2), BowTie Plus (CyberSec4Europe Deliverable D3.1, Section 5.2), PKI service (CySiMS) (CyberSec4Europe Deliverable D3.1, Section 7) and Secure AIS ASM endpoint (D3.1, Section7)	Develop and implement monitoring techniques that will analyse the data, and vulnerability databases providing efficient indexing. Explore, map and address risks related to unwanted maritime security events through the generation of bow-tie diagrams.
Challenge 4	Maritime system communication security	PKI service (CySiMS) (CyberSec4Europe Deliverable D3.1, Section 7), Secure AIS ASM endpoint (D3.1, Section7) and BowTie Plus (D3.1, Section 5.2)	Development of a targeted trust infrastructure. A PKI service provision to support encryption requirements to safeguard data AIS and VDES communication
Challenge 5	Securing autonomous ships	PKI service (CySiMS) (CyberSec4Europe Deliverable D3.1, Section 7), MITIGATE (D3.1, Section 5.4) and BowTie Plus (CyberSec4Europe Deliverable D3.1, Section 5.2)	Model threats against securing maritime autonomous surface ships (MASS). Develop risk models capable of addressing heterogeneous part of autonomous ships.

Table 3-22: CyberSec4Europe - Challenges and Tools in the Maritime Transport Vertical

The timeframe for the Incident Reporting vertical (as taken from CyberSec4Europe Deliverable D4.4)⁵¹ is provided below.

Maritime Transport Vertical - Roadmap Timeframe:
<p>12-month plan: Concerning the research challenge (Challenge 1: Early identification and assessment of risks, threats and attack paths for critical maritime systems):</p> <ul style="list-style-type: none"> <i>Achieved goals:</i> We have already worked on developing methodologies and tools to procure stable datasets. Furthermore, an initial consolidated structure of a risk assessment methodology, including threat calculation, vulnerability assessment and threat model identification, has been developed in the context of work for T5.5, based on the MITIGATE methodology. This methodology, along with the respective tools, is capable of providing a

Maritime Transport Vertical - Roadmap Timeframe:

method for attack path generation that aims to evaluate the propagation of threat events and to calculate risks to individual and cumulative values. In this respect, visualization techniques have been provided to demonstrate asset network graphs, attack graphs and risk reports, while diagrams are additionally available. At the same time, we have enhanced the existing risk assessment methodology with **evidence-based and scenario-based risk assessment approaches**, based on recent cybersecurity incidents that encapsulate sophisticated attacks and provided supporting threat scenarios to satisfy active learning processes (i.e. problem-based and case-based learning).

- *Expected goals:* In our updated 12-month plan, we plan to improve the cyber-attack path discovery algorithms that are capable of capturing the dependencies and interactions of maritime systems. Furthermore, we aim to improve the visualization techniques for illustrating **vulnerable attack paths and attack patterns**.

Concerning the research challenge (Challenge 2: Security hardening of maritime infrastructures, including cyber and physical systems):

- *Achieved goals:* Regarding system hardening, the initial plan included an analysis of available components for applying the necessary hardening techniques.
- *Expected goals:* In this aspect, we are in the position of having several different hardening techniques for instrumenting various forms of software (source, binary) and for different threats. The mapping of available solutions for instrumenting particular applications to mitigate specific threats will be integrated into the MITIGATE platform. Software hardening tools and solutions will be offered as new controllers in MITIGATE, which will be instantiated for specific threat classes. MITIGATE offers a classification of threats affecting different types of components. Not all threats can be countered using system hardening and not all components can be instrumented for security. Specifically, the plan for integrating all system hardening tools with MITIGATE is as follows:
 - We will enhance MITIGATE with new controllers for software hardening. Controllers are security components that can be effective in countering particular threats.
 - We will map all applications that are affected by threats addressable through hardening. Such threats are memory-corruption attacks, which can be used for exploiting native code.
 - Finally, we will enable the new controllers for the aforementioned threats.

Concerning the research challenge (Challenge 4: System communication security):

- *Achieved goals:* We have developed the necessary components for a trust infrastructure based on a PKI specifically configured for the limitations found in the maritime domain.
- *Expected goals:* We expect to achieve demonstrable integrations between maritime applications and the trust infrastructure. Furthermore, we seek to implement mechanisms for PKI certificate revocation that support ships in offline states and scale to a realistic number of clients (~100 000 – 200 000). We will implement a VDES-ready maritime communications application that emphasises the integrity, authenticity and privacy of messages.

2-year (or until the end of the project) plan

In the course of the next 2 years the research goals to be achieved are the following:

Concerning the research challenge (Challenge 1: Early identification and assessment of risks, threats and attack paths for critical maritime systems):

- We plan to experiment with enhancing the developed **cyber-attack path discovery algorithms** with novel machine learning techniques, or other computational models that are capable of capturing more accurately the dependencies and interactions of maritime systems.

Concerning the research challenge (Challenge 2: Security hardening of maritime infrastructures, including cyber and physical systems):

- The software hardening tools and solutions that will be integrated into the MITIGATE platform as new controllers will be further examined to improve their capacity and eliminate possible bugs or malfunctions.

Maritime Transport Vertical - Roadmap Timeframe:
<p>Concerning the research challenge (Challenge 4: System communication security):</p> <ul style="list-style-type: none"> In this context we aim to work towards offshore trials and standardization of a trust infrastructure that takes into consideration the environmental limitations of the maritime transport sector, such as network availability and communication costs. Since stability of communication is an issue, it is crucial to facilitate the availability and stability of communications solutions. Therefore, solutions need to be scalable and redundant. Within this context, a challenge to be met is to design and implement maritime systems that utilize both satellite and radio communication means. Given the need for stability and redundancy, such a design will partially address the need for achieving network availability in ship communications.
<p>Beyond the end of the project plan:</p> <p>The rest of the identified research challenges are expected to extend the lifetime of the project. In particular:</p> <p>Concerning the research challenge (Challenge 3: Resilience of critical maritime systems):</p> <ul style="list-style-type: none"> Ensuring the robustness of the maritime ICT infrastructures as well as quickly identifying and adapting to security threats are long-term research goals. They entail the development and implementation of monitoring techniques supported by AI algorithms that will analyse the data, and vulnerability databases that will ensure its better indexing. Part of this challenge is addressed by the tools to be developed for the risk assessment challenge. <p>Concerning the research challenge (Challenge 4: System communication security):</p> <ul style="list-style-type: none"> Integrating the VDES-ready secure communications application with the hardware (VDES devices) once the VDES standard has been finalized and the hardware becomes more available for use. <p>Concerning the research challenge (Challenge 5: Securing autonomous ships):</p> <ul style="list-style-type: none"> All the research goals identified under this research challenge are research goals that go beyond the lifetime of the project. However, it is expected that some of these goals will benefit from the advances produced by the other research goals. For example, the long-term goal for unified security and safety risk management of heterogeneous components in autonomous ships is expected to benefit from the development of stable data sets for the maritime environment, such as the targeted threat models. The secure 5G and satellite integration for ship connectivity in autonomous ships will take advantage of the development of secure maritime systems for dual satellite and radio communication needs. The goal for a comprehensive communication architecture for autonomous ships as well as the goal for GNSS security are expected to benefit from the development of a targeted trust infrastructure.

Table 3-23: CyberSec4Europe- Maritime Transport Timeframe

3.4.2.6 CyberSec4Europe Vertical – EU Medical Data Exchange

CyberSec4Europe identifies five challenges identified in the area of **Medical Data Exchange**, as follows:

- Challenge 1: Security and privacy
- Challenge 2: Mechanisms for preserving user data privacy
- Challenge 3: Trustworthiness on the data exchange platform
- Challenge 4: Accomplish regulation during the data sharing process
- Challenge 5: Data exchange platform user experience

The following Figure is the CyberSec4Europe Summary of their SWOT Analysis for the **Medical Data Exchange** vertical (as taken from CyberSec4Europe Deliverable D4.4⁵¹):



Figure 3-17: CyberSec4Europe – Medical Data Exchange SWOT Analysis Summary

The tools required for each challenge and the methods that need to be addressed are given in Table 3-23 (as taken from CyberSec4Europe Deliverable D4.4⁵¹).

Challenge	Tools required for	Tools contemplated for Medical Data Exchange	Tools/Methods that need to be addressed
Challenge 1	Security tools	SPeIDI (CyberSec4Europe Deliverable D3.1, Section 5.1), SS-PP IdM (D3.1, Section 5.1)	Secure shared data space infrastructure with access control
Challenge 2	Privacy-preserving assets	DANS (CyberSec4Europe Deliverable D3.1, Section 5.1) Crypto-FE (D3.1, Section 7), PLEAK (D3.1, Section 5.2)	Privacy preserving infrastructure
Challenge 3	Trust mechanisms	SPeIDI (CyberSec4Europe Deliverable D3.1, Section 5.1), SS-PP IdM (D3.1, Section 5.1) DANS (D3.1, Section 5.1) Crypto-FE (D3.1, Section 7)	Trust in shared data space infrastructure
Challenge 4	Regulation accomplish	Guidelines for GDPR compliant user experience (CyberSec4Europe D3.1, Section 5.6), and general-purpose	Adaptation data sharing scenarios
Challenge 5	User experience	Visualization tool developed in the context of T5.6 by Dawex	Graphical representation

Table 3-24: CyberSec4Europe: Challenges and Tools in the Medical Data Exchange Vertical

The timeframe for the Medical Data Exchange vertical (as taken from CyberSec4Europe Deliverable D4.4⁵¹) is provided below.

Medical Data Exchange Vertical - Roadmap Timeframe:
<p>12-month plan: This section provides an update of the developed activities considering the research challenges. The plan during the next 12 months includes the following activities:</p>

Medical Data Exchange Vertical - Roadmap Timeframe:

Privacy preserving assets. To complete the implementation and operation of the anonymization service (DANS) created for addressing the security and privacy challenges. The DANS asset is offered in two flavours: DANS as a service and as a library. On the one hand, the anonymization can be offered to the data providers by the Covid-19 Data Exchange³²¹ platform as an additional service. On the other, data providers can integrate the DANS library into their own system. These two options facilitate the performance of the anonymization process by the data providers, assuring that data privacy is preserved.

Additionally, initial steps for the use of a DPIA tool have been taken in order so that it can be applied to the data exchange platform during the next 12 months. The first steps for designing Crypto-FE have also been developed.

It is expected that the design, implementation and deployment of Crypto-FE asset will be finalized over the next twelve months.

Security tools and trust mechanisms. As planned, initial contacts with France Connect have been made in order to integrate the proxy eIDAS connector (SPeIDI), developed under the CyberSec4Europe project umbrella, with the France Connect system. For the next iteration of the Medical Data Exchange demonstrator, the integration of the exchange platform with the France Connect system through the SPeIDI asset is envisaged. The scope and duration of this integration will be limited, depending on the level of permission the French authority will provide for using the France Connect system.

Regulation accomplished. Initial contacts have been made with UM, the owner of the GDPR guidelines asset.

User experience. In response to the appearance of Sars-Cov-2 in our lives and the spread of the Covid-19 pandemic across the world, Dawex launched the initiative of the Covid-19 exchange platform, which aims to facilitate the work of researchers and health administrations by facilitating data sharing related to the coronavirus dissemination. In this new context, visualization and data assessment tools have been provided. For the next 12 months' period the refinement of these assets will be carried out.

2-year (or until the end of the project) plan:

Until the end of the project the plan for addressing the challenges provided as follows.

Regarding the **security, trust and privacy** tools:

- **Finalize the eIDAS network integration** with the Covid-19 Data Exchange platform.
- Perform **the integration of the Crypto-FE asset** for assuring end-to-end encryption between data providers and data consumers.
- **Set the basis for the adoption** (depending on the availability and maturity of assets) of a **decentralized access** to the platform based on the SSI paradigm.
- **Design the activities** to be implemented after the DPIA is performed. In addition, fix any issues that may arise during the integration of the described assets.
- **Provide guidelines** that describe, apart from the use of the assets developed during the project, how the adoption of these assets by data exchange platforms available to data providers and data consumers will increase security, trust and privacy when sensitive data are shared. The lessons learnt during the development of the Medical Data Exchange demonstrator could be extended to other data exchange domains.

Regarding the **regulation challenge** included in section 8.7.4, the envisaged plan described in document D4.3 [Markatos 2020]⁵⁰ is confirmed:

- "In order to produce the GDPR guidelines, the regulation, best practices and opinions provided by the European Commission and different supervisory authorities will be reviewed

Medical Data Exchange Vertical - Roadmap Timeframe:
<p>to create a comprehensive guideline, for use in as many situations and circumstance as possible.</p> <ul style="list-style-type: none"> • Additionally, research on regulatory matters and related tools will seek out ways for easier and better compliance with regulations such as GDPR and eIDAS. • An analysis of interoperability and cross-border compliance of the eIDAS compliant electronic identification, security and authentication services will be performed to identify flaws and compatibility of solutions between member States.” [Markatos 2020]
<p>Beyond the end of the project plan: The proposed activities to be developed after the project ends will be in line with the final results and the lessons learnt during the performance of the Medical Data Exchange demonstrator. The plans provided in D4.3⁵⁰ still apply at this moment, but will be updated depending on the final results of the demonstrator validation [Markatos 2020].</p> <ul style="list-style-type: none"> • “Dawex will provide a hybrid data exchange platform, with blockchain capabilities and functionalities for identity management (to be determined in phase 2), the decentralized exchange of data (currently being developed; will not be available for phase 1), and smart contracts (available). • These hybrid capabilities allow the parties supplying and sourcing the data, as well as the operator of the data exchange platform, to choose between two operating modes for managing the actual transfer of data, and the related payment when transactions are monetized. The decentralized mode takes advantage of the blockchain to allow the exchange to take place without an intermediary, while providing maximum trust, traceability and transparency, addressing the challenges of the healthcare market. • When considering data exchange the future of healthcare appears to be implantable medical devices. These are usually very small devices and are consequently limited (in their hardware, and consequently security capabilities). To protect the exchange of data and extend the lifetime of such devices, a new suite of light protocols for authentication, key exchange and possibly even encryption should be designed.” [Markatos 2020].

Table 3-25: CyberSec4Europe- Medical Data Exchange Timeframe

3.4.2.7 CyberSec4Europe Vertical – Smart Cities Vertical

CyberSec4Europe identifies ten challenges in the area of **Smart Cities**, as follows:

- Challenge 1 Trusted Digital Platform
- Challenge 2: Cyber threat intelligence and analysis platform
- Challenge 3: Cyber competence and awareness program
- Challenge 4: Privacy by design
- Challenge 5: Cyber response and resilience
- Challenge 6: End user trusted data management
- Challenge 7: Interoperability between legacy and new systems
- Challenge 8: Cyber fault/failure detection and prevention
- Challenge 9: Logging and monitoring
- Challenge 10: Information security and operational security

The following Figure is the CyberSec4Europe Summary of their SWOT Analysis for the **Smart Cities** vertical (as taken from CyberSec4Europe Deliverable D4.4⁵¹):



Figure 3-18: CyberSec4Europe – Smart Cities SWOT Analysis Summary

The tools required for each challenge and the methods that need to be addressed are given in Table 3-26 (as taken from CyberSec4Europe Deliverable D4.4⁵¹).

Challenge	Tools required	Tools contemplated for Smart Cities	Tools/Methods that need to be addressed
Challenge 1	Trusted Platform Digital	<ul style="list-style-type: none"> • SPeIDI (CyberSec4Europe Deliverable D3.1, Section 5.1) • Mobile p-ABC (D3.1, Section 5.1) • eiDASBrowser (D3.1, Section 5.1) • DynSmaug (D3.1, Section 5.4) • VCUCIM (D3.1, Section 5.4) • EEVEHAC (D3.1, Section 5.5) 	Incident Handling and Digital Forensics Network and Distributed Systems Software and Hardware Security Engineering
Challenge 2	Cyber threat intelligence and analysis platform	<ul style="list-style-type: none"> • Threat Intelligence Integrator (D3.1, Section 5.3) 	Legal Aspects Governance aspects of management, recovery, and continuity Information security
Challenge 3	Cyber competences and awareness program	<ul style="list-style-type: none"> • TO4SEE (CyberSec4Europe Deliverable D5.2, Section 8.2.3.2) 	A campaign from the public administration to improve the cyber competences and awareness of the citizens will be useful.
Challenge 4	Privacy by design	<ul style="list-style-type: none"> • GENERAL_D (D3.1, Section 5.1) • PPIdM (D3.1, Section 5.1) • PLEAK (D3.1, Section 5.2) • CaPe (D5.2, Section 8.2.3.2) 	Trust Management and Accountability. The WP3 and WP5 tools cover 5 of the 7 seven “Privacy by Design” principles. The following ones need to be addressed beyond the project:

Challenge	Tools required	Tools contemplated for Smart Cities	Tools/Methods that need to be addressed
			<ul style="list-style-type: none"> • full functionality with full privacy protection; • privacy protection through the entire lifecycle of the data.
Challenge 5	Cyber response and resilience	<ul style="list-style-type: none"> • Briareos (CyberSec4Europe Deliverable D3.1, Section 5.3) • RATING (D5.2, Section 8.2.3.2) 	Theoretical Foundations Identity Management
Challenge 6	End user trusted data management	<ul style="list-style-type: none"> • PPIIdM (D3.1, Section 5.1) • DANS (D3.1, Section 5.1) • PLEAK (D3.1, Section 5.2) • CaPe (D5.2, Section 8.2.3.2) • ARGUS (D3.11, Section 5.9) • PTASC (D3.11, Section 5.8) 	Data usage control Privacy concerns, behaviours, and practices Human aspects of trust User acceptance of security policies and technologies Auditing and accountability procedures
Challenge 7	Interoperability between legacy and new systems	<ul style="list-style-type: none"> • SPeIDI (D3.1, Section 5.1) • PTASC (D3.11, Section 5.8) • eIDASBrowser (D3.1, Section 5.1) 	Legal Aspects Network and Distributed Systems Formal verification of security assurance Software and Hardware Security Engineering Theoretical Foundations
Challenge 8	Cyber fault/failure detection and prevention	<ul style="list-style-type: none"> • Briareos (D3.1, Section 5.3) • RATING (D5.2, Section 8.2.3.2) 	Theoretical Foundations
Challenge 9	Logging and monitoring	<ul style="list-style-type: none"> • CaPe (D5.2, Section 8.2.3.2) 	Auditing and accountability procedures for personal data management in compliance with GDPR
Challenge 10	Information security and operational security	<ul style="list-style-type: none"> • Mobile p-ABC (D3.1, Section 5.1) • DynSmaug (D3.1, Section 5.4) • VCUCIM (D3.1, Section 5.4) • EEVEHAC (D3.1, Section 5.5) 	Network and Distributed Systems Software and Hardware Security Engineering

Table 3-26: CyberSec4Europe Challenges and Tools in Smart Cities

The timeframe for the Smart Cities vertical (as taken from CyberSec4Europe Deliverable D4.4)⁵¹ is provided below.

Smart Cities Vertical - Roadmap Timeframe:
<p>12-month plan: Trusted digital platform. Complete the privacy-preserving authentication and authorization framework by adding range proving and pseudonymity, plus complete integration with the</p>

XACML policy management also taking into account specifications from the current privacy regulations, in particular GDPR (e.g., consent management, etc..).

Cyber threat intelligence and analysis platform. For the next 12 months of the project, the SC demonstrator will integrate cyber-threat intelligence and analysis platforms, taking special account of automation and knowledge sharing, in order to increase the effectiveness of defences among stakeholders that share their cyber-threat intelligence. For this purpose, the pilot will integrate an MISP instance that retrieves cyber-threat information from compromised situations. End-users' devices and devices from the pilot infrastructure will gather this information and send it to the MISP instance. Finally, the CTI will share it among other MISP instances from the CS4E project.

Information security and operational security. For the next 12 months, the SC demonstrator will integrate information and operational security within cyber threat intelligence tools. In order to avoid the misuse of information, data will be protected using cryptographic approaches such as CP-ABE, while the privacy of involved entities is still preserved.

Privacy by design and end-user trusted data management. User centric transparency tools will be analysed from a user experience and usability point of view, aiming at a high degree of interoperability with the existing systems of SCs. In the next 12 months, the integration of CaPe (Consent Manager) and GENERAL_D tools for leveraging the SC, with automatic enforcing of GDPR provisions, into executable access control policies will be also finalized. Additionally, testing features will be designed for 1) evaluating the effectiveness of test strategies for the validation of GDPR-based access control policies; 2) testing the GDPR-based access control policies against GDPR requirements; and 3) assessing the GDPR compliance of the access control mechanisms.

Cyber response and resilience The integration of Briareos will allow integrating with TIPS provided by other partners' from the consortium, enhancing the devices' resilience when they are deployed in heterogeneous contexts and scenarios susceptible to attacks.

Interoperability between legacy and new systems. The possible expansion of the user base, thanks to the adoption of the eIDAS regulation, is stimulating LPA to identify in the short term the areas in which investment should be made in the redesign of online systems; in some cases, it will be sufficient to integrate the current legacy authentication systems (for example SIRAC SSO for Genova demonstrator) with eIDAS, while for other systems it will be necessary to proceed with the adaptation of the entire system, including data and internal logic, following the now widespread model of interoperability, in order to allow access to all interested European citizens.

Cyber competence and awareness program. We plan to work, in collaboration with WP6, on providing gamification methodologies and tools to assess and improve cyber competences and cyber-related capabilities for human aspects with respect to phishing attacks. As reported in the last Threat Landscape by ENISA [ENISA 2020B], phishing attacks represent one of the top 15 cyber threats nowadays; thus, we are moving in the right direction.

Logging and monitoring. We plan to extend the granularity and categories of events in the personal data processing processes that occur among data requestors and data sources (Data Controller and Processors), and data subjects. These events will be collected and managed in a user-centric manner by the CaPe solution. We plan to investigate, in collaboration with WP3 activities, techniques to guarantee non-repudiation and immutability of event logs through the adoption of distributed ledger solutions. In a DLT context, event log metadata may require that personal data and references have to be hashed rather than embedded in the ledger.

2-year (or until the end of the project) plan:

Risk assessment. Following the PDCA methodology described in section 9.7.1 (Integrated Security Risk Framework), we will process the DO phase: using the results of the PLAN phase that has just ended, we will perform all the activities needed to resolve the issues that have emerged. The outcomes to be analysed come from the cybersecurity risk assessment tool.

Privacy by design. For the remaining 2 years of the project, specific features will be provided for leveraging SCs with the automatic enforcing of the GDPR provisions within executable access and usage control policies. Additionally, specific features will be conceived in order to: 1) evaluate the effectiveness of test strategies for the validation of GDPR-based access control policies; 2) test the GDPR-based access control policies against GDPR requirements; and 3) assess the GDPR compliance of the access control mechanisms. During the last years, all the provided features will be assembled into a unique framework that can easily be integrated into the SC environment.

Cyber response and resilience. We plan to analyse the results of the first round of penetration testing. We will then perform the activities needed to resolve the issues that have emerged.

Trusted Digital Platform. For the SC demonstration case, we plan to integrate trusted digital platforms tools provided by the partners' consortium. These platforms will provide authentication, user transparency, data protection and data anonymization.

Cyber threat intelligence and analysis platform. For the remaining 2 years of the project, we should be moving towards a mature implementation, taking special account of automation and knowledge sharing, in order to increase the effectiveness of defences among stakeholders that share their cyber-threat intelligence. Finally, during the third year, the full integration should be able to provide a set of defined use cases. Thus, testing will be performed to check and verify the performance of the solution.

Cyber response and resilience. The integration of Briareos will allow integrating with TIPS provided by other partners' from the consortium, enhancing the devices' resilience when deployed in heterogeneous contexts and scenarios susceptible to attacks.

End user trusted data management. As digital identities become increasingly important, it is worth considering how a data management infrastructure can be made more trustworthy, empowering users whilst increasing the availability of data and ensuring citizens' safety and privacy. The plan will examine novel technologies and cutting-edge ideas in relation to how to build such a trust infrastructure, in particular the development of blockchain privacy-preserving approaches in the context of self-sovereign identity, taking into account aspects related to end-user acceptance and usability. The Porto demonstrator's challenges focus on data processing in a context that presents limited computational, network and storage resources. Aligned with the characteristics discussed, such as interoperability and heterogeneity, these features meet IoT analytics' major challenges. For the remaining 2 years of the project, we will focus on integrating with PTASC to ensure that users can share information without risk, but also allow them to sell the information generated in the SC in a trusted manner. ARGUS will allow devices to connect to a remote server where they can securely control the personal information generated and stored in multiple public cloud providers.

Interoperability between legacy and new systems. In the Porto pilot, PTASC will allow the city demonstrator to have devices to communicate end to end, independently of the architecture. In the Genoa pilot, thanks also to the AGID guidelines, which strongly push the use of eIDAS to replace SPID level 2 and 3, LPA plan to integrate online services (whose interest also extends to non-Italian citizens) with the new European authentication system, thus giving a new impulse to the economy and social inclusion.

Cyber fault/failure detection and prevention. From the point of view of prevention, the analysis of the cyber-risk self-assessment will offer the opportunity to find out which are the

main cyber threats in the SC environment. Our plan is to make them evident to the municipality, highlighting possible mitigation actions to carry out good prevention.

Information security and operational security. To address this challenge, for the next 2 years, it is necessary to continue integrating widely used encryption and access control mechanisms. In the end, the pilot will produce a use case that combines privacy with analysis, exchange and creation of a knowledge database on cyber threats.

Beyond the end of the project plan:

It is obviously a complex problem to imagine what will happen after the end of the project, considering the speed with which SCs are evolving today. However, it is reasonable to think that the solutions provided by the CyberSec4Europe project will be taken over by software houses, which will have the task of customizing them and distributing them among their current and potential customers.

Some challenging aspects that can be addressed after the end of the project are:

- **Ensure full participation of stakeholders:** because in the SC environment the most important (and numerous) stakeholders are citizens. To win people's trust and involvement will be a long process, but successful cases like London, Amsterdam and Paris, and the small Reykjavík project [IESE 2019], demonstrate that a real change can be made in people's minds
- **Adapt governance structures:** this aspect could be affected by the typical resistance to changes in public administration, due to the bureaucratic processes needed to perform any governance innovation. For this reason, it is more realistic to think that it will be a long process.
- **Interoperable solutions:** transporting the IT infrastructure of an LPA into the SC environment involves the adoption of interoperable solutions that are not always already available in the IT assets. It is for this reason that it is necessary to work to make all systems interoperable, starting from those considered strategic, to guarantee a smart service increasingly felt as necessary by citizens who in the SC nourish hope for a new model of life that will also be eco-sustainable. To guarantee all this, it will be necessary for these new IT infrastructures to adopt security requirements more and more intimately, because it becomes essential to guarantee citizens that their digital identity, and therefore also their data in the LPAs, is complete and inviolable. With these bases in the field of IT security it will be possible to build more and more of what is called SC.

3.4.3 ECHO

Website: <https://echonetwork.eu/>

ECHO focuses on development of cybersecurity technology roadmaps resulting from an analysis of current emerging cybersecurity challenges and associated technologies. In total, six inter-sector technology roadmaps are foreseen, two of which are technology roadmaps with the aim to describe future (inter sector) opportunities for the development of ECHO Federated Cyber Range (E-FCR) and the ECHO Early Warning System (E-EWS) which will be delivered as part of the project. The purpose of the E-FCR and E-EWS technology roadmaps is to present future development options aiming for the continuous improvement, adaptation and evolution of the ECHO platforms after the end of the project and when the CCN will be active.

The roadmaps aim to create the foundations for new industrial capabilities and assist in the development of innovative technologies that will aim to address these cybersecurity challenges.

ECHO Deliverable D4.3 “Inter-sector cybersecurity technology roadmap”⁵⁴, which describes E-FCR and E-EWS, was published in August 2020 and addresses the following objectives:

- “Demonstration of a network of cyber research and competence centres with a central competence hub, having a mandate for increasing participation through a new partner engagement model, including collaboration with other networks funded under the same call.
- Address current cybersecurity EU gaps. Development of an adaptive model for information sharing and collaboration among the network of cybersecurity centres supported by an early warning system and a framework for improved cyber skills development and technology roadmap delivery, in a multiple-sector context

The goal of E-FCR is to interconnect existing cyber-range capabilities through a portal operating as a broker between user requirements and a pool of available cyber range capabilities. The objective of the E-FCR is to solve the problem of simulation of the complex realities and inter-sector dependencies of an inter-sector scenario by establishing a mechanism by which the independent cyber-range capabilities can be interconnected and accessed via a convenient portal for configuration and management.

The five major domains in E-FCR capture different aspects of technology, environment and requirements evolution, as follows:

- **User experience** domain deals with how users of the Cyber Ranges and E-FCR interact with the tools
- **Connectivity** domain explores effect of future connectivity development
 - **5g challenges:**
 - Constantly increasing the attack surface
 - Cross device dependencies
 - Access to IoT devices
 - Negative effects of complexity and connectivity
- **Scalability** discusses ways to scale the E-FCR platform
- **Platform** domain deals with Cyber Ranges platforms and integration
- **Exploitation** domain focuses on novel uses of the E-FCR platform

An important aspect in the development of the above are the user stories, with a total of 29 user stories identified and developed for the two roadmaps.

One of the main benefits of implementation of E-FCR will be to address the challenge of “Lack of cyber situational awareness in national critical infrastructure and gaps in defense in-depth architecture hacking.”

The goals of the ECHO Early Warning System (E-EWS) within ECHO are:

- “Deliver a secure sharing support tool enabling personnel to coordinate and share cyber-sensitive information in near real-time.
- Support information sharing across organizational boundaries and between disparate information repositories as may be used by partner organisations, including granular control of data and functionality access.
- Provide sharing capability of both general cyber information and specific incident management data.

⁵⁴ ECHO Deliverable 4.3 “Inter-sector cybersecurity technology roadmap” https://echonetwork.eu/wp-content/uploads/2020/11/ECHO_D4.3-INTER-SECTOR-CYBERSECURITY-TECHNOLOGY-ROADMAP-v1.0.pdf

- Secure connection management from clients accessing the E-EWS, to ensure only personnel with a valid certificate can access E-EWS functions and data.
- The secure information sharing model will account for sector-specific needs including GDPR compliance and others related to health care, banking, insurance and other sectors dealing with personal data.”

For E-EWS, the three major domains which capture different aspects of technology, environment and requirements evolution are:

- **User experience** domain deals with how users of the EWS interact with the platform
- **Platform domain** deals with how the EWS can be grown and integration of new tools
- **Exploitation domain** focuses on uses and adoption of the E-EWS platform

The ECHO roadmaps will be updated in January 2023 (M48 of ECHO project), as D4.10 “Update – Inter-sector cybersecurity technology roadmap” and will incorporate additional technology roadmaps.

3.4.4 SPARTA

Website: <https://www.sparta.eu/>

The Strategic Programs for Advanced Research and Technology in Europe (SPARTA) published in February 2020 its updated roadmap:

SPARTA Deliverable D3.2 - “Updated SPARTA SRIA (Roadmap v1)”⁵⁵

SPARTA’s roadmap emerged from a set of 60 seed challenges in research and innovation. From these challenges, four programs were launched, specifically:

- Full spectrum cybersecurity awareness (T-SHARK),
- Continuous assessment in polymorphous environments (CAPE),
- High-assurance Intelligent infrastructure toolkit (HAIL-T),
- Secure and fair AI for the Citizens (SAFAIR).

In addition to the four SPARTA Program Challenges, transversal challenges and emerging challenges are also considered in the Roadmap.

The SPARTA Roadmap is updated periodically and is designed to be agile and open in order to consider emerging trends and technologies and other areas which may arise out of discussions with SPARTA partners and community.

A top-level glimpse of the SPARTA Roadmap Timeline (as taken from SPARTA Deliverable 3.2⁵⁵) with the goals is given in Figure 3-19 with the final goals in solving the identified challenges. Figure 3-20 presents a detailed description of the sub-goals of existing programs and other work packages pursued by SPARTA and a timeline showing the 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.

SPARTA’s Roadmap D3.2 (Jensen) (February 2020): <https://www.sparta.eu/assets/deliverables/SPARTA-D3.2-Updated-SPARTA-SRIA-roadmap-v1-PU-M12.pdf#page=61>

The timelines provided combine the dimensions of *technology*, *education*, and *certification* and align SPARTA's short- and midterm goals with these domains. The short- and midterm goals consider a timeline until the official end of SPARTA. However, the timeline also includes SPARTA's long term goals that go beyond the official end of SPARTA.

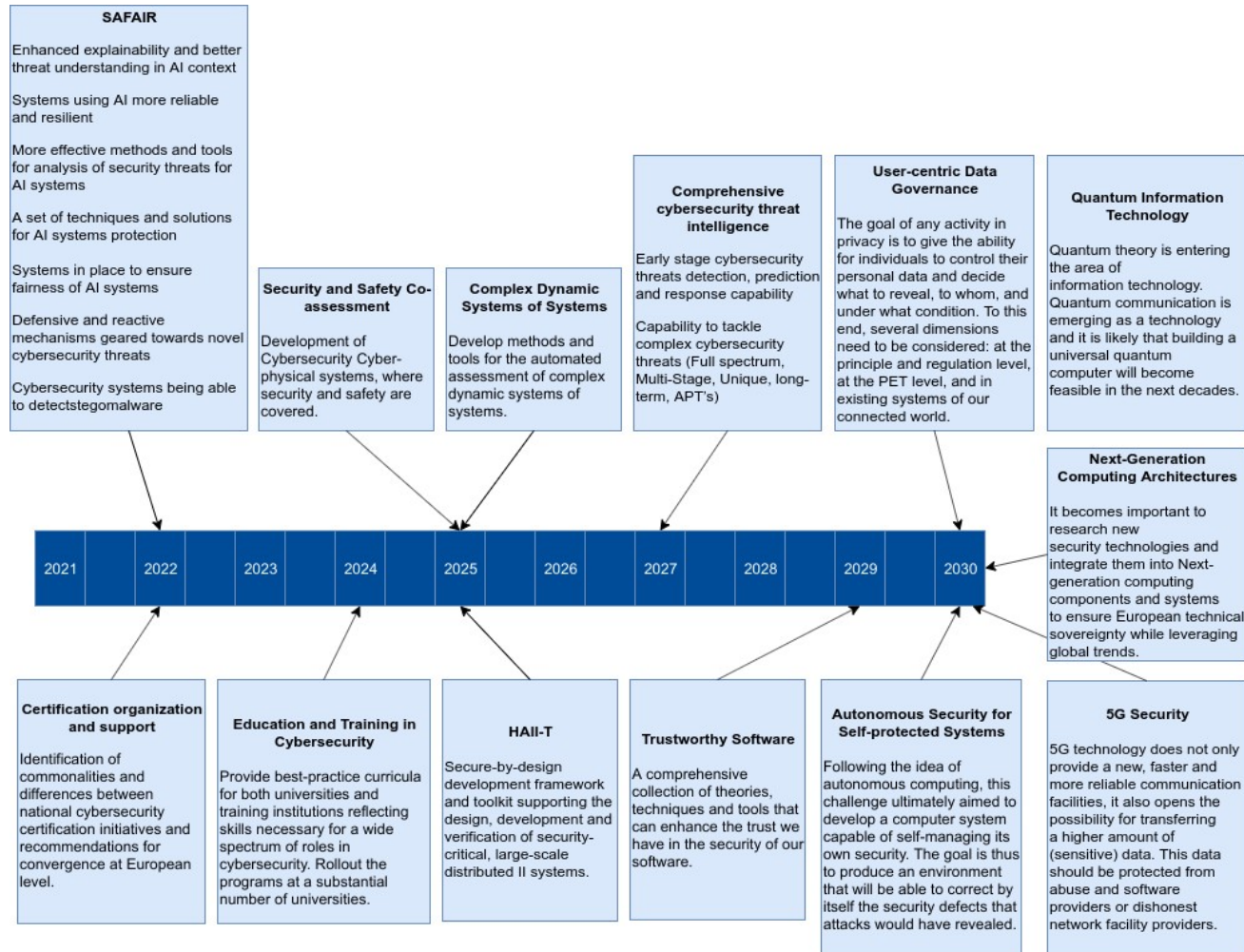


Figure 3-19: SPARTA Roadmap with the final goals to solve identified challenges

D3.2 - Updated SPARTA SRIA (Roadmap v1)

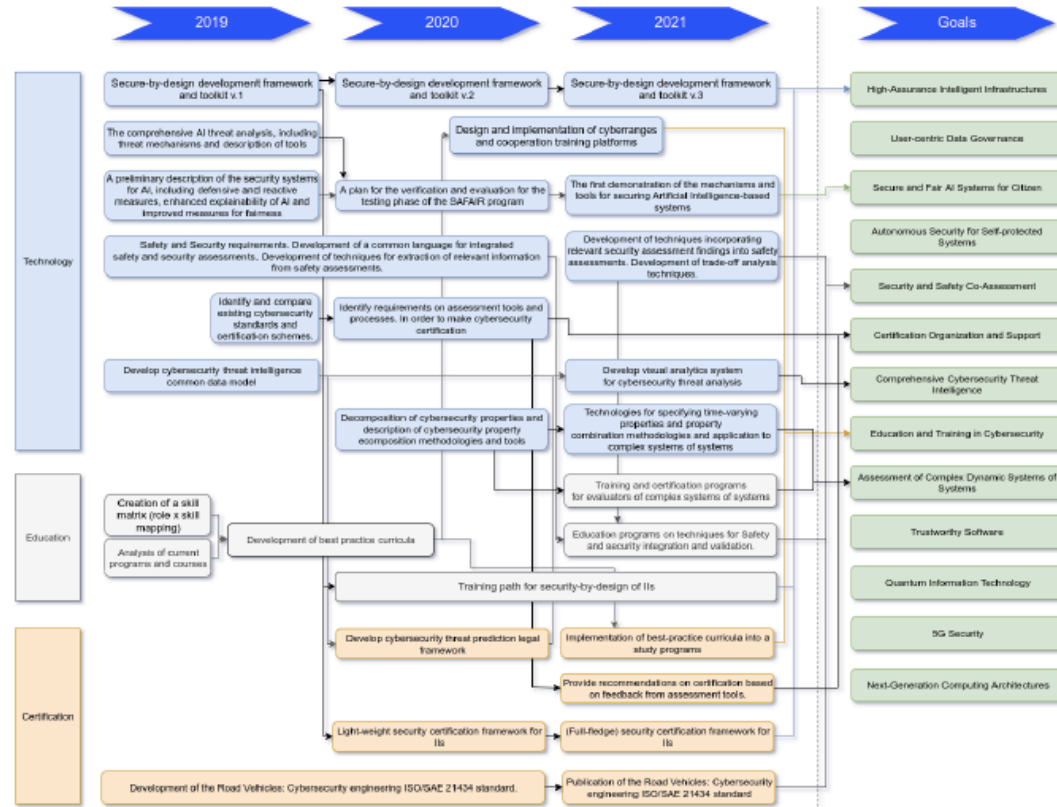


Figure 2: Timeline of stages for technology, education and certification

Figure 3-20: SPARTA Timeline of stages for technology, education and certification

Within each program, a set of challenges is defined with a description of:

- the problem, trends, risks and market opportunities, and a SWOT analysis
- the final goal, status quo, estimated year of completion,
- the research and social aspects, industry demands, benefits for the EU
- its relation to emerging challenges,
- the applicable JRC taxonomy (domain, sector)

Within each challenge, there are a set of sub-goals defined which are further combined with the dimensions of Technology, Education and Certification. A timeline for the expected completion of each activity with a top-level description of the sub-goal is given follows (as taken from SPARTA Deliverable 3.2⁵⁵):

3.4.4.1 T-SHARK — Full-Spectrum Situational Awareness

The T-SHARK Program in SPARTA means to establish a Full-Spectrum Cybersecurity Threat Intelligence Framework by developing comprehensive solutions based on novel technology developments and cross-disciplinary breakthroughs. T-Shark will develop and validate methodological, organizational and technological solutions extending cybersecurity towards comprehensive organization of security functions, enabling threat prediction and full-spectrum cybersecurity awareness, providing high situational awareness, informing decision and policy makers on broad or long-term issues and/or providing a timely warning of threats. It will expand the reach of threat understanding, from current investigative-level definition, up to strategic considerations on current, future and down to real-time events handling and prevention. It will allow in near future to establish EU cybersecurity capability to predict complex cyber threats and prevent them before damage appeared.⁵⁶

The SWOT analysis for this challenge is given below (as extracted from SPARTA Deliverable 3.2⁵⁵):

SPARTA SWOT Analysis: Comprehensive Cybersecurity Threat Intelligence
<p>Strengths:</p> <ul style="list-style-type: none"> • Meeting actual demand • Realistic to implement and achieve • High support by end-users <p>Weaknesses:</p> <ul style="list-style-type: none"> • Demands for large scale information access • Organized around the “Threats” concept, that is new and has little of regulatory and legal frameworks <p>Opportunities</p> <ul style="list-style-type: none"> • 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 <p>Threats</p> <ul style="list-style-type: none"> • Many of innovative aspects tipping together that increases the risk of failure

Table 3-27: SPARTA SWOT Analysis for Comprehensive Cybersecurity Threat Intelligence

⁵⁶ Description about T-SHARK from <https://www.sparta.eu/programs/t-shark/>

Figure 3-21 provides a timeline for the completion of the stages in Comprehensive Cybersecurity Threat Intelligence (from T-SHARK) (as taken from SPARTA Deliverable 3.2⁵⁵).

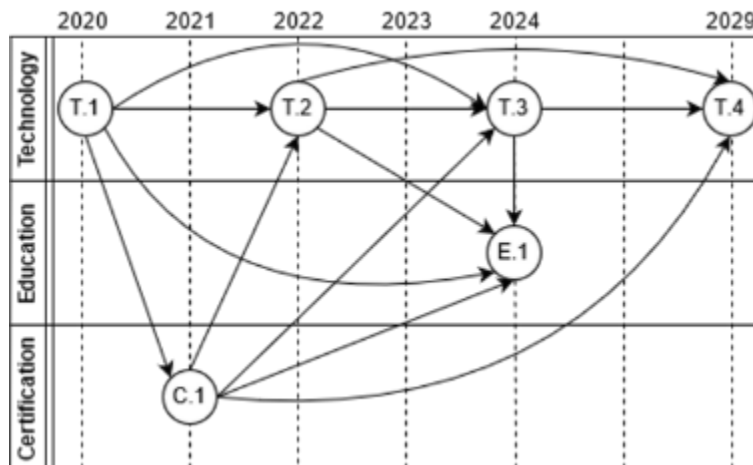


Figure 3-21: SPARTA Timeline for expected completion of Comprehensive Cybersecurity Threat Intelligence (from T-SHARK)

Sub-goals	Description
T1	Develop Cybersecurity threat intelligence common data model.
T2	Develop Visual Analytics System for Cybersecurity threat analysis.
T3	Develop cybersecurity threat analysis model.
T4	Develop comprehensive full-spectrum cybersecurity threat intelligence methodology.
E1	Education programs on the basis of comprehensive full-spectrum cybersecurity threat intelligence methodology.
C1	Develop cybersecurity threat prediction legal framework.

Table 3-28: SPARTA – Sub-goals in Comprehensive Cybersecurity Threat Intelligence

3.4.4.2 Continuous Assessment in Polymorphous Environments (CAPE)

The CAPE program provides its input to the SPARTA Roadmap through two separate challenges:

- **Security and Safety Co-Assessment** which focuses on complexity and dynamicity of IT systems of systems, where the main issue is to adapt assessment processes to dynamicity and complexity, and
- **Assessment of Complex Dynamic Systems of Systems**, which focuses on resilience of the physical world, embedding both security and safety features into physical components controlled through IT processes.

Currently, it is felt that the two challenges are sufficiently different to provide separate roadmap descriptions but, in the future, the approach may change.

3.4.4.2.1 Security and Safety Co-Assessment

As described in SPARTA Deliverable D3.2:

“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.”

The SWOT analysis for Security and Safety Co-Assessment is given below (as extracted from SPARTA Deliverable D3.2):

SPARTA SWOT Analysis: Security and Safety Co-Assessment	
Strengths:	<ul style="list-style-type: none"> Existing research activities in the EU
Weaknesses:	<ul style="list-style-type: none"> 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:	<ul style="list-style-type: none"> Concrete guarantees for safety and security, certain use cases (e.g., connected vehicle) are applicable to major industries in Europe
Threats:	<ul style="list-style-type: none"> Major actors in the digital transformation (GAFAM) are developing and experimenting with these technologies

Table 3-29: SPARTA SWOT Analysis for Security and Safety Co-Assessment

The SPARTA Timeline for the expected completion of sub-goals for Security and Safety Co-Assessment is given in Figure 3-22 (as taken from SPARTA Deliverable 3.2⁵⁵).

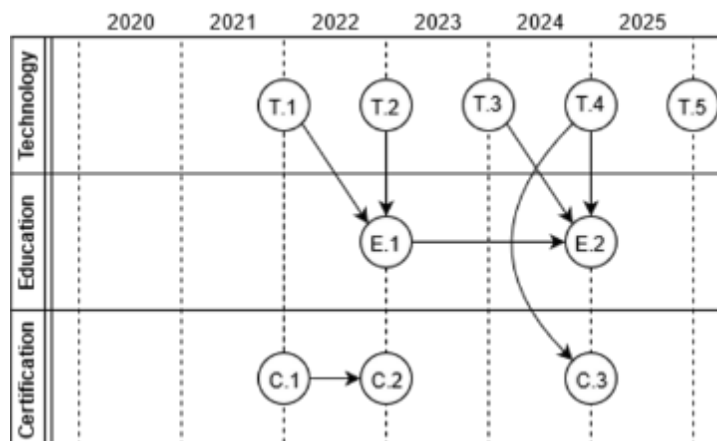


Figure 3-22: SPARTA Timeline for the expected completion of sub-goals for Security and Safety Co-Assessment (from CAPE)

Sub-goals	Description
T1	Safety and Security requirements.

T2	Development of techniques incorporating relevant security assessment findings into safety assessments.
T3	Development of safety and security co-verification and validation techniques.
T4	Develop incremental methods for safety and security integration.
T5	Continuous safety and security assessment process.
E1	Education programs based on Safety and Security assessment.
E2	Education programs on techniques for Safety and Security integration and validation.
C1	Development of the Road Vehicles: Cybersecurity engineering ISO/SAE 21434 standard.
C2	Publication of the Road Vehicles: Cybersecurity engineering ISO/SAE 21434 standard.
C3	Development a methodology to assess safety and cybersecurity of systems.

Table 3-30: SPARTA – Sub-goals in Security and Safety Co-Assessment

3.4.4.2.2 Assessment of Complex Dynamic Systems of Systems

As described in SPARTA Deliverable D3.2:

“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 behaviour
- Assessment of service interdependencies
- Assessment towards certification of systems and services “

The SWOT analysis for Assessment of Complex Dynamic Systems of Systems is given below (as extracted from SPARTA Deliverable D3.2):

SPARTA SWOT Analysis: Assessment of Complex Dynamic Systems of Systems
Strength:

<ul style="list-style-type: none"> Existing software products and services providers <p>Weaknesses:</p> <ul style="list-style-type: none"> Lack of unified certification schemes <p>Opportunities:</p> <ul style="list-style-type: none"> Development of new schemes for certification taking into account the new EU certification framework <p>Threats:</p> <ul style="list-style-type: none"> Unstable regulatory environment
--

The SPARTA Timeline for the expected completion of sub-goals for the Complex Dynamic Systems of Systems is given in Figure 3-23 (as taken from SPARTA Deliverable 3.2⁵⁵).

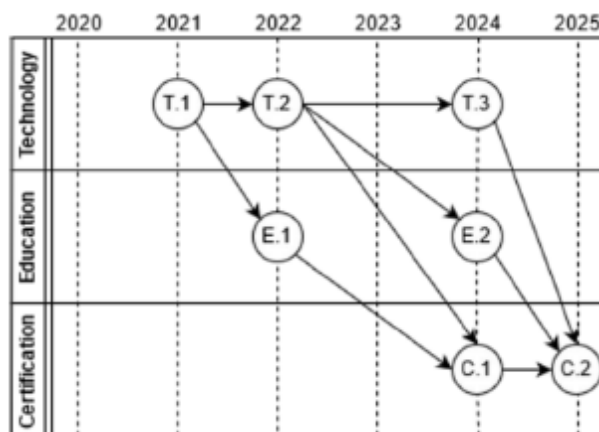


Figure 3-23: SPARTA D3.2 - Expected completion sub-goals for Complex Dynamic Systems of Systems (from CAPE)

Sub-goals	Description
T1	Decomposition of cybersecurity properties and description of cybersecurity property decomposition methodologies and tools.
T2	Technologies for specifying time-varying properties and property combination methodologies and application to complex systems of systems.
T3	Technologies for specifying time-varying properties driven by algorithms (e.g., AI, ML) and property combination methodologies for complex services.
E1	Training and certification programs for evaluators of complex systems of systems.
E2	Training and certification programs for evaluators of complex services, including dynamic services driven by AI/ML techniques.
C1	Evaluation scheme for complex systems of systems.
C2	Evaluation scheme for complex dynamic services.
C3	Development a methodology to assess safety and cybersecurity of systems.

Table 3-31: SPARTA D3.2 – Sub-goals in Complex Dynamic Systems of Systems (from CAPE)

3.4.4.3 High-Assurance Intelligent Infrastructure Toolkit – HAIIT

As described in SPARTA Deliverable D3.2:

“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.”

The SWOT analysis for the High-Assurance Intelligent Infrastructure Toolkit is given below (as extracted from SPARTA Deliverable D3.2):

SPARTA SWOT Analysis: High-Assurance Intelligent Infrastructure Toolkit	
Strengths:	
<ul style="list-style-type: none"> • Many EU research institutions are already working on the development of techniques that will contribute to the solution. 	
Weaknesses:	
<ul style="list-style-type: none"> • Poor security in components. 	
Opportunities:	
<ul style="list-style-type: none"> • Strengthening the industry by providing tools for the secure-by-design development of IIs. 	
Threats:	
<ul style="list-style-type: none"> • Integration of different techniques is challenging. The computational complexity of privacy-enhancing technologies. 	

The SPARTA Timeline for the expected completion of sub-goals for the High-Assurance Intelligent Infrastructures is given in Figure 3-24 (as taken from SPARTA Deliverable 3.2⁵⁵).

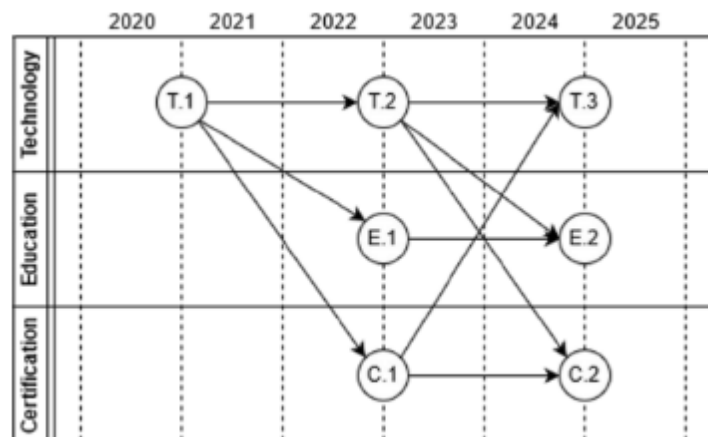


Figure 3-24: SPARTA D3.2 - Expected completion sub-goals for High-Assurance Intelligent Infrastructures (from HAI-T)

Sub-goals	Description
T1	HAI-T secure-by-design development framework and toolkit v.1.
T2	HAI-T secure-by-design development framework and toolkit v.2.
T3	HAI-T secure-by-design development framework and toolkit v.3.
E1	HAI-T training path for security-by-design of IIs (target: designers and developers of IIs).
E2	HAI-T training path for security-by-design of IIs (target audience: scientists and engineers interested in the development and extension of the HAI-T framework).
C1	HAI-T light-weight security certification framework for IIs.
C2	HAI-T (full-fledge) security certification framework for IIs.

Table 3-32: SPARTA D3.2- Sub-goals in High-Assurance Intelligent Infrastructures (from HAI-T)

3.4.4.4 SAFAIR — Secure and Fair AI Systems for the Citizen

As described in SPARTA Deliverable D3.2:

“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.”

The SWOT analysis for the Secure and Fair AI Systems for the Citizen is given below (as extracted from SPARTA Deliverable D3.2):

SPARTA SWOT Analysis: Secure and Fair AI Systems for the Citizen

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

The SPARTA Timeline for the expected completion of sub-goals for Secure and Fair AI Systems for Citizen is given Figure 3-25.

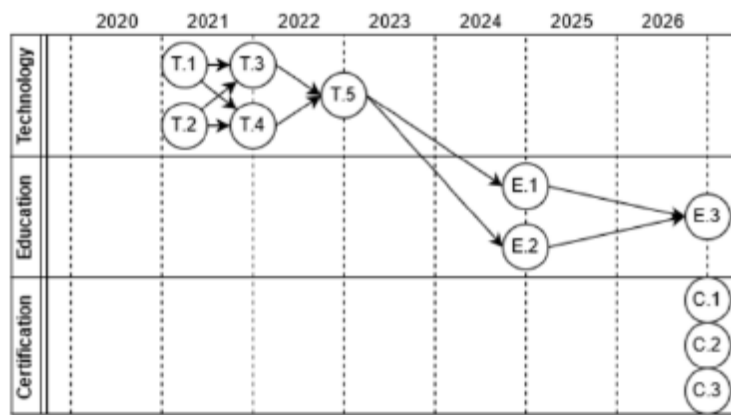


Figure 3-25: SPARTA D3.2 - Expected completion sub-goals for Secure and Fair AI Systems for Citizen (from SAFAIR)

Sub-goals	Description
T1	The comprehensive AI threat analysis, including threat mechanisms, novel threats in cybersecurity and AI, and description of necessary tools.
T2	A preliminary description of the security systems for AI, including defensive and reactive measures, enhanced explainability of AI and improved measures for fairness.
T3	A plan for the verification and evaluation for the testing phase of the SAFAIR program.
T4	The first demonstration of the mechanisms and tools for securing Artificial Intelligence-based systems.
T5	The final version of security mechanisms and tools for AI systems.
E1	The SAFAIR secure AI educational program, explaining the threats of adversarial learning along with the defensive and reactive measures.
E2	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	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.

Sub-goals	Description
C1	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	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	THE SAFAIR SEAL OF APPROVAL - A certification geared towards the venues utilizing AI, proving the utilized algorithms are secure, explainable and fair.

Table 3-33: SPARTA D3.2 - Sub-goals for Secure and Fair AI Systems for Citizen (from SAFAIR)

3.4.4.5 Education and Training in Cybersecurity

As described in SPARTA Deliverable D3.2

“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.”

The SWOT analysis for Education and Training in Cybersecurity is given below (as extracted from SPARTA Deliverable D3.2):

SPARTA SWOT Analysis: Education and Training in Cybersecurity
<p>Strengths:</p> <ul style="list-style-type: none"> • Good experience in the consortium, some programs already rolled out, good practice from non-EU countries. <p>Weaknesses:</p> <ul style="list-style-type: none"> • 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. <p>Opportunities:</p> <ul style="list-style-type: none"> • No EU-level best practices for education exist now, strong demand in the job market for experts in cybersecurity. <p>Threats:</p> <ul style="list-style-type: none"> • Curricula are not widely accepted by institutions, new programs are not accepted at national levels (e.g., due to accreditation processes)

The SPARTA Timeline for the expected completion of sub-goals for Education and Training in Cybersecurity is given in Figure 3-26 (as taken from SPARTA Deliverable 3.2⁵⁵).

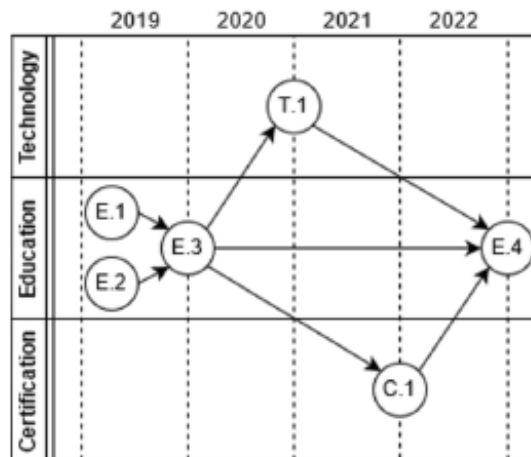


Figure 3-26: SPARTA D3.2 - Expected completion sub-goals for Education and Training in Cybersecurity

Sub-goals	Description
T1	Design and implementation of cyber ranges and cooperation training platforms.
E1	Creation of a skill matrix (role x skill mapping).
E2	Analysis of current programs and courses.
E3	Development of best practice curricula.
E4	Pilots with real students.
C1	Implementation of best-practice curricula into a study program, including accreditation and certification (where possible).

Table 3-34: SPARTA D3.2 – Sub-goals for Education and Training in Cybersecurity

3.4.4.6 Certification Organization and Support

As described in SPARTA Deliverable D3.2:

“Problem description: Given the growing threats that connected systems face, it has become important to protect IT-based infrastructures and systems sufficiently. Cybersecurity certification is one way to help engineers design more secure systems. Over the years, many cybersecurity standards and certifications schemes have been created at both European and international level. In the context of the European digital single market, it is important to have a simple cybersecurity certification scheme that is recognized throughout all European countries. To move in this direction there is a need to analyse different national European cybersecurity initiatives as well as international efforts in order to identify commonalities and differences. Standards and certification schemes can be classified in different ways. Some standards and schemes have been designed for products and others for processes and services. Other standards are sector-specific such as in transport or aeronautics. Others focus on specific technologies, e.g., networks or cloud computing. More widespread adoption of cybersecurity certification in the design of connected products and services will be successful only if certification is perceived as cost-effective and that it effectively improves the quality of products and services. For certification to be more widely adopted in security engineering, there is a clear need to design more agile certification processes, to better integrate certification in the security engineering process, and to improve the effectiveness of certification schemes.

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

The SWOT analysis for Certification Organization and Support - Mapping of international and European cybersecurity certification - is given below (as extracted from SPARTA Deliverable D3.2):

SPARTA SWOT Analysis: Certification Organization and Support - Mapping of international and European cybersecurity certification	
Strengths:	
<ul style="list-style-type: none"> • Cybersecurity certification is a topic of interest for all European countries due to the NIST directive 	
Weaknesses:	
<ul style="list-style-type: none"> • There is a lot of divergence currently between member state approaches 	
Opportunities:	
<ul style="list-style-type: none"> • The EU cybersecurity act is an opportunity to make national and international cybersecurity certification schemes converge more. 	
Threats:	
<ul style="list-style-type: none"> • Pushing for more cybersecurity certification can be costly and could have an impact on the competitiveness of European products and services. 	

The SPARTA Timeline for the expected completion of sub-goals for Certification Organization and Support is given in Figure 3-27 (as taken from SPARTA Deliverable 3.2⁵⁵).

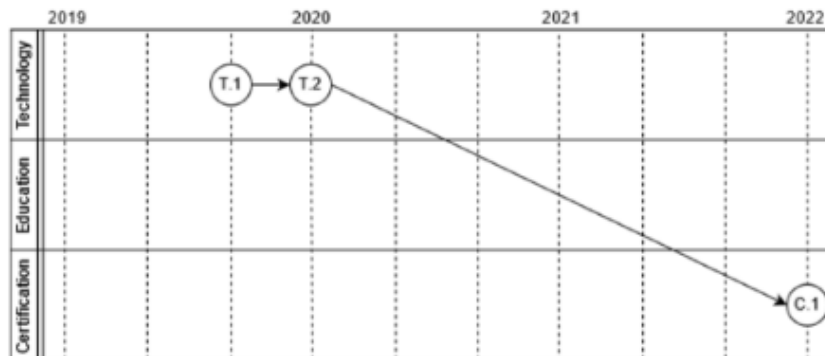


Figure 3-27: SPARTA D3.2- Expected completion sub-goals for Certification Organization and Support

Sub-goals	Description
T1	Identify and compare existing cybersecurity standards and certification schemes.
T2	Identify requirements on assessment tools and processes. In order to make cybersecurity certification.
C1	Provide recommendations on certification based on feedback from the assessment tools developed in the CAPE research program.

Table 3-35: SPARTA D3.2 – Sub-goals for Certification Organization and Support

3.4.4.7 User-Centric Data Governance

As described in SPARTA Deliverable D3.2:

“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 behaviours, which requires data flow analyses, is hindered by the number, complexity, and diversity of underlying applications and communication technologies. Challenging transverse research activities are required to bring transparency, highlight good and bad practices, and enable regulators to enforce data protection laws.

Final goal: The goal of any activity in privacy is to give the ability for individuals to control their personal data and decide what to reveal, to whom, and under what condition. To this end, several dimensions need to be considered: at the principle and regulation level, at the PET level, and in existing systems of our connected world.”

The SWOT analysis for User-Centric Data Governance is given below (as extracted from SPARTA Deliverable D3.2):

SPARTA SWOT Analysis: User Centric Data Governance
<p>Strengths:</p> <ul style="list-style-type: none"> • Privacy is a highly accepted European value both by politicians and by citizens, and is supported by high-level academic research. <p>Weaknesses:</p> <ul style="list-style-type: none"> • 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. <p>Opportunities:</p> <ul style="list-style-type: none"> • The GDPR application and high awareness of threats against privacy are excellent signs. <p>Threats:</p> <ul style="list-style-type: none"> • 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).

The SPARTA Timeline for the expected completion of sub-goals for User Centric Data Governance is given in Figure 3-28 (as taken from SPARTA Deliverable 3.2⁵⁵).

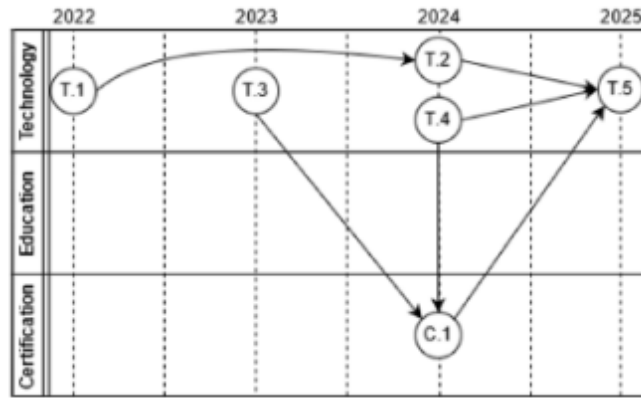


Figure 3-28: SPARTA D3.2 - Expected completion sub-goals for User-Centric Data Governance

Sub-goals	Description
T1	Privacy protection technologies and tools.
T2	Analysis of privacy threats and attacks.
T3	Privacy Evaluation.
T4	Privacy-preserving management and regulations.
C1	Evaluation / certification of privacy in applications and systems.

Table 3-36: SPARTA D3.2 - Sub-goals for User-Centric Data Governance

3.4.4.8 Autonomous Security for Self-Protected Systems

As described in SPARTA Deliverable D3.2:

“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.”

The SWOT analysis for Autonomous Security for Self-Protected Systems is given below (as extracted from SPARTA Deliverable D3.2):

SPARTA SWOT Analysis: Autonomous Security for Self-Protected Systems
<p>Strengths:</p> <ul style="list-style-type: none"> • 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. <p>Weaknesses:</p> <ul style="list-style-type: none"> • This is a highly risked research topic. Success is by no means guaranteed. <p>Opportunities:</p> <ul style="list-style-type: none"> • Autonomous security is not currently operative. This is a subject on which Europe could take the research and then industrial lead. <p>Threats:</p> <ul style="list-style-type: none"> • The automation of the attack (e.g., offensive AI) could be operational before that of the defense.

The SPARTA Timeline for the expected completion of sub-goals for Autonomous Security for Self-Protected Systems is given in Figure 3-29 (as taken from SPARTA Deliverable 3.2⁵⁵).

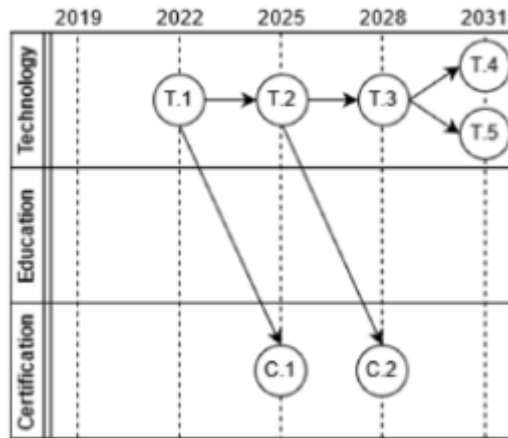


Figure 3-29: SPARTA D3.2 - Expected completion sub-goals for Autonomous Security for Self-Protected Systems

Sub-goals	Description
T1	Properly define the system's security policy and how it is implemented.
T2	Detect violations of security policies in real-time.
T3	Accurately diagnosing the causes and sources of security policies violations.
T4	Automatically propose changes to the policy and/or its implementation
T5	Recovering the attacked system.
C1	Detecting intrusions and anomalies: toward controlled false positive and false negatives rates.
C2	Ensure that the defensive response to attacks is relevant.

Table 3-37: SPARTA - Sub-goals for Autonomous Security for Self-Protected Systems

3.4.4.9 Trustworthy Software

As described in SPARTA Deliverable D3.2:

“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”.

The SWOT analysis for Trustworthy Software is given below (as extracted from SPARTA Deliverable D3.2):

SPARTA SWOT Analysis: Trustworthy Software
<p>Strengths:</p> <ul style="list-style-type: none"> Strong academic level; successes in some industrial sectors <p>Weaknesses:</p> <ul style="list-style-type: none"> Some strong industrial EU stakeholders (Thales, SAP, Leonardo, Indra, etc.) but no global and worldwide undisputed leadership. <p>Opportunities:</p>

- 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.

The SPARTA Timeline for the expected completion of sub-goals for Trustworthy Software is given in Figure 3-30 (as taken from SPARTA Deliverable 3.2⁵⁵).

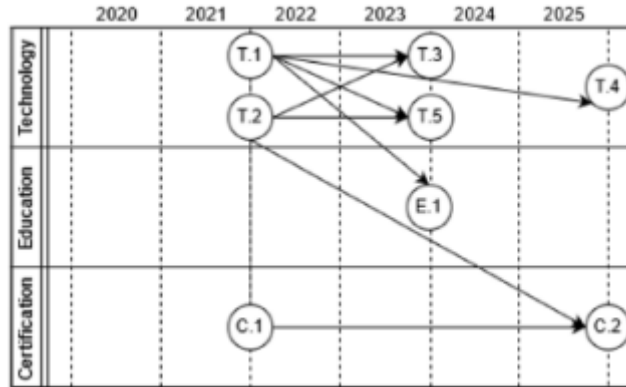


Figure 3-30: SPARTA D3.2 - Expected completion sub-goals for Trustworthy Software

Sub-goals	Description
T1	Model-driven engineering of secure software.
T2	Binary analysis. Develop static and dynamic analysis techniques for analyzing binary code.
T3	Evaluation and hardening of legacy code.
T4	Explore the use of proof assistants and automatic software verification for validating security properties.
T5	Malware analysis. Develop static and dynamic analysis techniques for identifying malware based on its behavior, improving on today’s signature-based techniques.
E1	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	Make evolve existing certification schemes to take into account recent advances in formal methods-based techniques.
C2	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 3-38: SPARTA D3.2 – Sub-goals for Trustworthy Software

3.4.4.10 Quantum Information Technology

As described in SPARTA Deliverable D3.2:

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

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

The SWOT analysis for Quantum Information Technology is given below (as extracted from SPARTA Deliverable D3.2):

SPARTA SWOT Analysis:	
Strengths:	<ul style="list-style-type: none"> Strong knowledge of European research community in quantum information technologies and quantum cryptography. Acknowledgement of its importance by the high governmental agencies
Weaknesses:	<ul style="list-style-type: none"> Many international (mostly American) corporates invest much higher amount of money into the development of quantum information technologies than Member States and EU, in general. Some of these companies demonstrate better progress with respect to the EU.
Opportunities:	<ul style="list-style-type: none"> It is of paramount importance to possess the knowledge of quantum information technologies, as it may impact all spheres of life. This also means huge market demand (in the nearest future) for the quantum information solutions.
Threats:	<ul style="list-style-type: none"> Loosing the quantum race. Underinvestment. Brain drain and technology leakage (e.g., by corporates who buy technology and people).

The SPARTA Timeline for the expected completion of sub-goals for Quantum Information Technology is given in Figure 3-31 (as taken from SPARTA Deliverable 3.2⁵⁵).

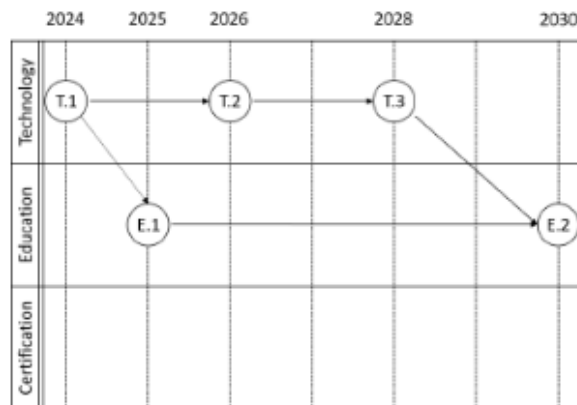


Figure 3-31: SPARTA D3.2 - Expected completion sub-goals for Quantum Information Technology

Sub-goals	Description
T1	Quantum communication and secure key distribution.
T2	Post-quantum cryptography.
T3	Security of computing platforms mixing classical and quantum computation.
E1	Quantum and post quantum cryptography professionals.
E2	A new generation of (cyber) security professionals should be raised with the knowledge of both quantum theory and information technology.

Table 3-39: SPARTA D3.2 - Timeline for expected completion of sub-goals for Quantum Information Technology

3.4.4.11 5G Security

As described in SPARTA Deliverable D3.2:

“Problem description: 5G technology does not only provide a new, faster and more reliable communication facilities, it also opens the possibility for much higher amount of (sensitive) data to be transferred, connecting different types of infrastructure and applying novel technologies. These data should be protected from the possible abuse by malicious technology and software providers or dishonest network facility providers.

Final goal: Although a number of issues should be solved, in order to ensure adequate protection for the new communication technology, the overall goal could be stated as to protect the data during its transmission via 5G networks.”

The SWOT analysis for 5G is given below (as extracted from SPARTA Deliverable D3.2):

SPARTA SWOT Analysis: 5G	
Strengths:	<ul style="list-style-type: none"> Strong knowledge of the European (academic and industrial) community in security policies, security management, communication security, intrusion detection and malware analysis, security engineering, etc. Some EU companies are developing their own 5G network technologies. A strong European research community informal methods, security policies, reasoning and logic, intrusion detection and alert correlation. Some industrial key actors in the security business.
Weaknesses:	<ul style="list-style-type: none"> European technologies for 5G is lagging behind the most advanced companies from US and China.
Opportunities:	<ul style="list-style-type: none"> The 5G technology market is promised to be huge and will be operational only in the nearest future.
Threats:	<ul style="list-style-type: none"> Superiority of the current 5G leaders could be very hard to catch up with. Moreover, the major investments and human resources could be attracted by the leading (non-EU) companies.

The SPARTA Timeline for the expected completion of sub-goals for 5G is given in Figure 3-32 (as taken from SPARTA Deliverable 3.2⁵⁵).

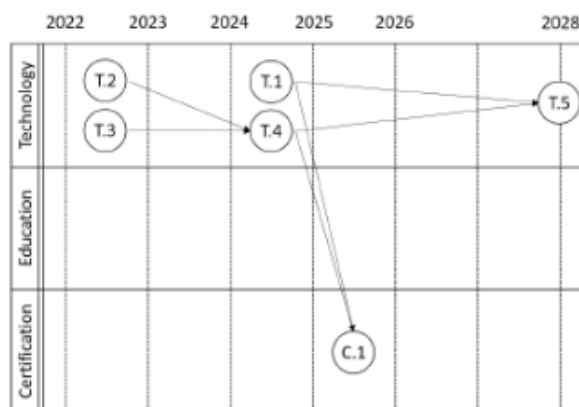


Figure 3-32: SPARTA D3.2 - Expected completion sub-goals of 5G Security

Sub-goals	Description
T1	Security orchestration and management.
T2	Resilience against flash of network traffic.
T3	End-to-end security (network and application level).
T4	Consistency of subscriber level of protection.
T5	Adaptive security (new technologies, new threats).
C1	Certification of 5G hardware and software.

Table 3-40: SPARTA D3.2 - Sub-goals of 5G Security

3.5 SPARTA Roadmaps Analysis

The SPARTA pilot has already carried out an exercise to analyse national strategies and project roadmaps. The analysis is found in SPARTA Deliverable D3.2⁵⁵. The information which follows is taken from SPARTA's analysis.

3.5.1 SPARTA Analysis of European Cybersecurity National Strategies

In its Roadmap SPARTA performed an analysis of some European cybersecurity national strategies which could influence the landscape at the national and European levels. Topics were identified according to their priority and, then, mapped according to JRC's taxonomy for cybersecurity and R&I. The following national strategies were analysed by Sparta in their Roadmap D3.2⁵⁵:

- Austria: Austrian Cyber Security Strategy (2013)
- Czech Republic: National Cyber Security Strategy (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 (2019)
- Germany: Selbstbestimmt und sicher in der digitalen Welt (Research program in federal government in IT security) 2015-2020 (2015)
- Greece (SPARTA partners provided direct input)
- Italy Libro Bianco (White Book) 2018
- Lithuania: National Cyber Security Strategy (2018)
- Luxembourg: National Cybersecurity Strategy III (2018)
- Poland: The National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022 (2017)
- Spain:
 - Spanish Industrial Cybersecurity Roadmap 2013 - 2018 (2013)
 - NCIBE: Market Trends in Cybersecurity (2016)

The results of this SPARTA analysis are provided in Table 3-41, Table 3-42 and Table 3-43.

3.5.2 National Roadmaps mapped to JRC Research Domains

In Table 3-41, SPARTA provides a mapping of some National Cybersecurity Roadmaps⁵⁵ to JRC’s Research Domains resulted with the following topics as being highly relevant:

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


D3.2 Updated SPARTA SRIA (Roadmap v1)													SPARTA	
	Spain Ind.	Austria	Czech	Germany	Spain	Poland	Italy	Lithuania	Luxembourg	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
 Table 3-41: SPARTA - Analysis of national cybersecurity roadmaps according to JRC’s research domains

3.5.3 National Roadmaps mapped to JRC Applications & Technologies

In Table 3-42, SPARTA provides a mapping of some National Cybersecurity Roadmaps⁵⁵ to JRC’s Applications and Technologies resulted in the following topics as being highly relevant:

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


SPARTA

D3.2 Updated SPARTA SRIA (Roadmap v1)

	Spain Ind.	Austria	Czech	Germany	Spain	Poland	Italy	Lithuania	Luxembourg	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

Table 3-42: SPARTA - Mapping of National Cybersecurity Roadmaps to JRC Applications & Technologies

3.5.4 National Roadmaps mapped to JRC Sectors

In Table 3-43, SPARTA provides a mapping of the national cybersecurity roadmaps to JRC Sectors and ranks the following topics as highly relevant:

- Health care
- Energy
- Transportation
- Financial

 SPARTA

D3.2 Updated SPARTA SRIA (Roadmap v1)

	Spain Ind.	Austria	Czech	Germany	Spain	Poland	Italy	Lithuania	Luxembourg	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

Table 3-43: SPARTA - Mapping of national cybersecurity roadmaps according to JRC Sectors

3.5.5 European Cybersecurity Project Roadmaps

In the SPARTA Roadmap Deliverable D3.2⁵⁷, SPARTA further carried out a mapping of European projects in order to obtain an analysis at the European level. For this purpose, SPARTA selected the following documents to be analysed:

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

The results of the analysis by SPARTA are provided in Table 3-44, Table 3-45, Table 3-46.

3.5.6 EU Project Roadmaps Mapped to JRC Research Domains

The analysis by SPARTA (Section 3.3.2 of SPARTA Deliverable D3.2) of European Cybersecurity Project Roadmaps according to JRC’s Research Domains resulted in the following as being highly relevant:

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

	NESSoS	TDL	SYSSEC	NIS WG3	cPPP	Camino	Aegle	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 3-44: SPARTA - Mapping of European Cybersecurity Roadmaps to JRC Research Domains

⁵⁷ SPARTA’s Roadmap <https://www.sparta.eu/assets/deliverables/SPARTA-D3.2-Updated-SPARTA-SRIA-roadmap-v1-PU-M12.pdf>

3.5.7 EU Project Roadmaps Mapped to JRC Appl. & Technologies

The analysis of SPARTA in its mapping of European Cybersecurity Project Roadmaps to JRC’s Applications and Technologies (Section 3.3.2 of SPARTA Deliverable D3.2) identified the following as highly ranked:

- Mobile devices
- Big data
- Cloud and Virtualization
- Blockchain and Distributed Leger Technology
- Internet of Things
- Operating Systems

 SPARTA

D3.2 Updated SPARTA SRIA (Roadmap v1)


	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 3-45: SPARTA - Mapping European Cybersecurity Roadmaps to JRC’s Applications and Technologies

3.5.8 EU Project Roadmaps Mapped to JRC’s Sectors

SPARTA’s mapping of European Cybersecurity Project Roadmaps to JRC’s Sectors (Section 3.3.2 of SPARTA Deliverable D3.2^{Error! Bookmark not defined.}) identified the following top sectors. These sectors were also identified by the national roadmap analysis of SPARTA (see Section 3.5.4):

- Health care
- Energy
- Transportation
- Financial


SPARTA

D3.2 Updated SPARTA SRIA (Roadmap v1)

	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 3-46: SPARTA - Mapping of European Cybersecurity Roadmaps to JRC Sectors

3.6 Joint Research Centre (JRC)

The European Commission's Joint Research Centre (JRC) is a department (Directorate-General, DG) of the European Commission providing independent scientific and technological support for EU policy-making. Most instrumental in the area of cybersecurity are the proposals and reports which follow, namely, the JRC Taxonomy, the European Cybersecurity Atlas, and the report “Cybersecurity – Our Digital Anchor”.

3.6.1 JRC Taxonomy

In 2019, the Joint Research Centre (JRC) released a technical report aiming to align the cybersecurity terminologies, definitions and domains to capture all the aspects in building the cybersecurity realm of knowledge.

This report presented some of the existing cybersecurity clustering approach and methodology that has been adopted to build the taxonomy which served as reference sources in the domain.

One of the stated reference sources is Cyberwatching.eu cybersecurity research taxonomy in which European projects, both national and international, are mapped, with the aim of clustering European Research and Innovation initiatives dealing with cybersecurity and privacy.

The **JRC** proposal consists of three-dimensional taxonomy based on the **cybersecurity domains** on

- (1) research,
- (2) sectorial and
- (3) technology and use case dimensions.

The taxonomy proposed in this document is that of supporting the mapping of the European **cybersecurity** competence available. The domains are reproduced in below:

Research Domains
Assurance, Audit and Certification
Cryptology (Cryptography and Cryptanalysis)
Data Security & Privacy
Education & Training
Human Aspects
Identity Management
Legal Aspects
Network & distributed systems
Security Management & Governance
Security Measurements
Software and Hardware Security Engineering
Steganography, Steganalysis and Watermarking
Theoretical Foundations
Trust Management and Accountability
Sectorial
Audiovisual and media
Chemical
Defence
Digital Services and Platforms
Energy
Financial
Food and drink
Government
Health
Manufacturing and Supply Chain
Nuclear
Safety and Security
Space
Telecomm Infrastructure
Transportation
Technologies and Use Cases Dimension
<ul style="list-style-type: none"> • Artificial Intelligence

<ul style="list-style-type: none"> • Big data • Blockchain and Distributed Ledger Technology (DLT) • Cloud, Edge and Virtualisation • Critical Infrastructure Protection (CIP); • Protection of public spaces • Disaster resilience and crisis management • Fight against crime and terrorism • Border and external security • Local/wide area observation and surveillance • Hardware technology (RFID, chips, sensors, networking, etc.) • High-performance computing (HPC); • Human Machine Interface (HMI) • Industrial IoT and Control Systems (e.g. SCADA and Cyber Physical Systems – CPS) • Information Systems • Internet of Things, embedded systems, pervasive systems • Mobile Devices • Operating Systems • Quantum Technologies (e.g. computing and communication) • Robotics • Satellite systems and applications • Vehicular Systems (e.g. autonomous vehicles) • UAV (unmanned aerial vehicles)
--

Table 3-47: JRC Taxonomy

Given the importance of the JRC taxonomy to the CS&P policy landscape, it was incorporated into the EU Project Radar meaning that users can use the radar to identify projects that are working on a particular technology or vertical sector covered by the three-dimensional taxonomy.

The radar quickly visualises the selections (including multiple) and provides aggregating statistics for all selected projects. Information displayed includes:

- Number of displayed projects
- Alphabetic list of funding calls
- Average project duration in months
- Total duration in years across all selected projects
- Average budget in € per budget
- Total budget in € across all selected projects

Using the live version of the radar we have been able to provide detailed information on the above information for each taxonomy element. This is included in Deliverable D2.7 “Technology Radar Final Report” Section 3.3. It should be noted that the taxonomy is additive, i.e. that the viewer is able to select multiple attributes to filter upon which can be used in either a summative or exclusive manner, i.e. you may select projects based on projects that have any one of the multiple attributes selected or you may select projects based on only those project that have all of the attributes selected.

3.6.2 European Cybersecurity Atlas

The **European Cybersecurity Atlas**⁵⁸ is a digital knowledge management and collaborative platform (<https://cybersecurity-atlas.ec.europa.eu/>) which aims to map, categorise and stimulate collaboration between cybersecurity experts across Europe.

cyberwatching.eu partners have disseminated the EU Project radar to the JRC for potential use as part of the Atlas.

3.6.3 The JRC Report “Cybersecurity – Our Digital Anchor – A European perspective”⁵⁹

The JRC Report “**Cybersecurity – Our Digital anchor – a European perspective**”⁵⁹ discusses re-orienting the approach of Europe to cybersecurity from a technical feature to a societal need that is included by-design in all products, processes and technologies, promoting resilience and adaptability. It calls for future actions on: ethics and rights, education, industry and digital services (standardization), greater research coordination, greater MS cooperation, emerging technologies.

3.7 Relevant Academic/Research Results

Overall, as has been shown from the analysis of the Cybersecurity R&I landscape as presented within Deliverable D2.7, the landscape is dominated (~45%) by projects that have been developing technology for any number of cybersecurity domains, the Secure Systems sector. Alongside this we have seen clear under representation of funded projects in the areas of cybersecurity that can be characterised as human factors, Governance and Verification and Assurance. This is especially worrying when considering that the ‘gateway’ for many cybersecurity breaches is a social engineering attack or similar. Overall though due to the COVID pandemic there is a clear break in the supply pipeline of projects that will create the Adoptable products of one or two years time. This is clearly shown in Figure 3-33 below, which illustrates 134 projects positioned within the radar compared to a high-water mark of 191 projects for Autumn 2019.

Notice that in this section we are analysing the Cybersecurity R&I landscape from the academic point of view, based exclusively on the projects’ lifecycle and domain, without taking into account the market readiness of the projects, which is described in Section 2.4.

⁵⁸ European Cybersecurity Atlas at <https://cybersecurity-atlas.ec.europa.eu/>

⁵⁹ JRC publication “Cybersecurity – our digital anchor – A European perspective” online at <https://publications.jrc.ec.europa.eu/repository/handle/JRC121051>

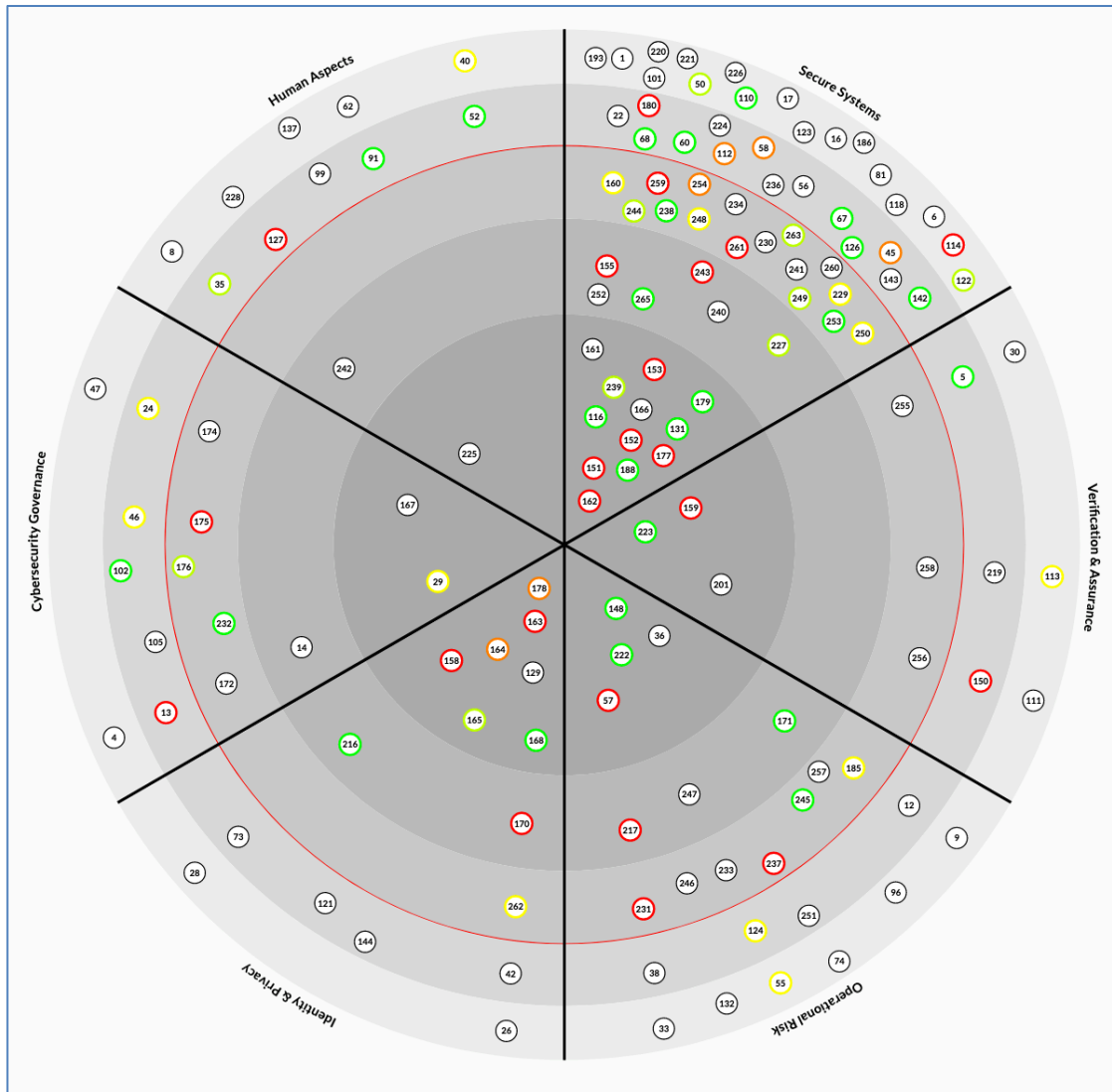


Figure 3-33 Cyberwatching Project Radar, Spring 2021

When looking at those projects within the cyberwatching.eu radar that have been tagged with the JRC taxonomy we can see that there is a clear balance between those projects that are tagged with relevant sub domains of Technology Sectors, Application Domains and Technology & use cases. The only concern with the analysis is that there are a number of lighthouse projects of significant size (>16M€) that can distort the analysis since they claim to participation in a significantly larger number of areas when compared with other projects. This is particularly important in the Verification and Assurance area where the single project consumes nearly 50% of all total funding in that area.

3.8 National Institute of Standards and Technology (NIST) - USA

The latest roadmap on privacy by the National Institute of Standards and Technology (NIST) aims to underline the areas of priority in evolving and advancing the evolution

of the NIST's Privacy Framework.⁶⁰ Within this roadmap, NIST introduces the key challenges posed to organizations that try to achieve their privacy objectives, and subsequently suggests a set of actions that must be taken in order to overcome these challenges. The NIST Roadmap is linked with their Privacy Framework, which is a voluntary tool intended to improve the privacy of businesses through risk management.⁶¹

In this section, the privacy roadmap will allow EU policy makers to clearly comprehend the future steps of improvement that NIST has identified within the context of their Privacy Framework. Although the roadmap includes the following eight areas of priority, NIST clarifies that this list is not exhaustive but is merely representative of input and feedback received from NIST's stakeholders:⁶²

3.8.1 Priority area 1: Privacy risk assessment

Initially, NIST emphasizes the importance of identifying and evaluating privacy risks, the process of a privacy risk assessment, in both developing effective solutions and in creating systems or products guaranteeing a higher protection of people's privacy.⁶³ However, based on the survey the NIST carried out the **risk assessment in the privacy sector is still under development**, with a lack of uniform concepts of privacy risk assessment.⁶⁴ In comparison to the cybersecurity domain, whereby a risk assessment is well established through commonly recognized risk models (including the factors of likelihood, vulnerability, threat and impact) it becomes clear that the resources in the privacy realm remain limited.⁶⁵ As a result, organisations are unable to effectively consolidate privacy risk assessments in their processes, which in hand results to a lack of general implementation of any actions to minimize privacy risks. Some necessary tools include a list of identified risk factors, as well as more in-depth guidance and tools for privacy risk assessments.

The underlying challenge that must be overcome in this priority area is the integration of privacy risk assessments to already existing risk management processes, such as cybersecurity risk assessments. In addition, evaluating the impact to persons whose data is being processed must be reflected within the organization in actionable ways. As a conclusion, NIST recognizes that more actions are necessary to reach a "common privacy risk model" which will also allow for more effective privacy risk assessment practices and implementation. For example, collaboration and engagement with stakeholders is necessary to integrate privacy into enterprise risk management guidance.⁶⁶

⁶⁰ Roadmap for Advancing the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise risk Management, January 16, 2020. Available at: <https://www.nist.gov/system/files/documents/2020/01/16/NIST-Privacy-Framework-Roadmap-v1.0.pdf>.

⁶¹ NIST Privacy Framework: A tool for improving privacy through enterprise risk management, version 1.0, January 16, 2020. Available at: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST-CSWP.01162020.pdf>, p.6.

⁶² Roadmap for Advancing the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise risk Management, January 16, 2020. Available at: <https://www.nist.gov/system/files/documents/2020/01/16/NIST-Privacy-Framework-Roadmap-v1.0.pdf>, p.1.

⁶³ NIST Privacy Framework: A tool for improving privacy through enterprise risk management, version 1.0, January 16, 2020. Available at: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST-CSWP.01162020.pdf>, p.6.

⁶⁴ Roadmap for Advancing the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise risk Management, January 16, 2020. Available at: <https://www.nist.gov/system/files/documents/2020/01/16/NIST-Privacy-Framework-Roadmap-v1.0.pdf>, p.5.

⁶⁵ NIST Summary Analysis of the Responses to the NIST Privacy Framework Request for Information, Available at: https://www.nist.gov/system/files/documents/2019/02/27/rfi_response_analysis_privacyframework_2.27.19.pdf, p.8.

⁶⁶ Roadmap for Advancing the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise risk Management, January 16, 2020. Available at: <https://www.nist.gov/system/files/documents/2020/01/16/NIST-Privacy-Framework-Roadmap-v1.0.pdf>, p.2.

3.8.2 Priority area 2: Mechanisms to provide confidence

Confidence in systems, products of services in privacy is the ability to demonstrate effective privacy protections. In spite of the fact that generally there is a range of mechanisms to provide such confidence (e.g., audits, inspections, testing, certification, etc.), the privacy domain has not yet determined a sufficient number of confidence mechanisms.⁶⁷ This lack thereof is an obstacle for companies because they must individually find confidence mechanisms, without any guarantee of their effectiveness. NIST suggests **supplementary research to this direction in order to better identify the challenges and needs of organisations regarding confidence mechanisms** for privacy; also indicating that the mechanisms of the cybersecurity sector can be relied on as possible examples.

In addition, NIST encourages **market-based approaches to increase confidence**. This recommendation is close to the goals of the Cyberwatching.eu project in bringing closer Research & Innovation products, solutions and services with stakeholders such as SMEs. To address the challenges in choosing an appropriate product or service to increase confidence in privacy, NIST recommends the collaboration of NIST stakeholders, including standards development organisations, in order to produce guidance or standards on assessment procedures or criteria for assessing marketable products and services with the aim of becoming confidence mechanisms.⁶⁸

3.8.3 Priority area 3: Emerging technologies

The third challenge to address is how to design systems, products and services that use emerging technologies, such as Internet of Things (IoT) and Artificial Intelligence (AI) and at the same time guarantee the protection of individual's privacy.⁶⁹ One of the main hurdles is understanding and managing the complexity of emerging technologies' data processing ecosystem. Therefore, **NIST identifies a need for research focusing on the development and integration of privacy guidance, standards, practices and tools to manage the complexities of emerging technologies.**⁷⁰

Further, NIST promotes research in the fundamental aspects that will allow organizations to better comprehend and manage privacy risks arising from emerging technologies, including the evaluation of bias and fairness. Moreover, privacy guidance must be integrated into IoT or AI guidance, tools, frameworks and standards in order to assist their implementation.

3.8.4 Priority area 4: De-identification risks and re-identification risks

The technique mitigating privacy risks posed to individuals through de-identification is a valuable method of protecting the privacy of persons while retaining the benefit of aggregate statistics. However, this technique includes a variety of technical implementations such as data masking, noise-introduction through differential privacy or synthetic datasets, which have not yet been fully embedded in the products

⁶⁷ Roadmap for Advancing the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise risk Management, January 16, 2020. Available at: <https://www.nist.gov/system/files/documents/2020/01/16/NIST-Privacy-Framework-Roadmap-v1.0.pdf>, p.2.

⁶⁸ Roadmap for Advancing the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise risk Management, January 16, 2020. Available at: <https://www.nist.gov/system/files/documents/2020/01/16/NIST-Privacy-Framework-Roadmap-v1.0.pdf>, p.2.

⁶⁹ Roadmap for Advancing the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise risk Management, January 16, 2020. Available at: <https://www.nist.gov/system/files/documents/2020/01/16/NIST-Privacy-Framework-Roadmap-v1.0.pdf>, p.2.

⁷⁰ Roadmap for Advancing the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise risk Management, January 16, 2020. Available at: <https://www.nist.gov/system/files/documents/2020/01/16/NIST-Privacy-Framework-Roadmap-v1.0.pdf>, p.3.

available in the market.⁷¹ Therefore, NIST finds that although the development of guidance, practices and tools for de-identification are emerging, it is still necessary to **increase the market-readiness and implementation of such tools.**

In addition, even if de-identification techniques are applied a possibility of re-identification remains. Therefore, it is essential that awareness is raised on the possibility of re-identification and promotion of methods to measure and mitigate the risks of re-identification. This could be done through collaboration with NIST stakeholders in order to both develop standards, guidance and tools on de-identification techniques as well as managing the risks of re-identification.⁷²

3.8.5 Priority area 5: Inventory and mapping

Inventory and data mapping is an activity that helps organizations identify and prioritize privacy risks, as well as illustrate the flow of the data processing. However, carrying out this activity in a precise manner can become burdensome for organizations when complex data processing environment are involved, large volumes of data, or different types of data (structured and unstructured).⁷³ As a result, NIST **asks for support of organizations through more guidance, best practices and automation tools to establish a cost-effective approach** in data inventory and mapping.

The activities that must be taken to this aim include engagement and collaboration with relevant stakeholders to understand the specific challenges they face and the subsequent development of the necessary tools in order to assist stakeholders' efforts in overcoming such challenges.

3.8.6 Priority area 6: Technical standards

NIST points out a lack of development in privacy-related technical and testing methodology standards. Technical standards are necessary in order for organizations to improve their ability to locate data and to respond to peoples' data management requests. Furthermore, standardized data formats can support the use of AI technologies as a mean to protect the privacy of individuals. Meanwhile standards for a testing methodology will strengthen the effectiveness of privacy protections.⁷⁴

Therefore, NIST identified the need to **collect information from relevant stakeholders in order to identify the topics where standardization is necessary.**

⁷⁵ In addition, the engagement with stakeholders is indispensable also for the standards' development in order to progress with **technical and assessment standards that support privacy engineering.**

⁷¹ Roadmap for Advancing the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise risk Management, January 16, 2020. Available at: <https://www.nist.gov/system/files/documents/2020/01/16/NIST-Privacy-Framework-Roadmap-v1.0.pdf>, p.3.

⁷² Roadmap for Advancing the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise risk Management, January 16, 2020. Available at: <https://www.nist.gov/system/files/documents/2020/01/16/NIST-Privacy-Framework-Roadmap-v1.0.pdf>, p.3.

⁷³ Roadmap for Advancing the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise risk Management, January 16, 2020. Available at: <https://www.nist.gov/system/files/documents/2020/01/16/NIST-Privacy-Framework-Roadmap-v1.0.pdf>, p.4.

⁷⁴ Roadmap for Advancing the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise risk Management, January 16, 2020. Available at: <https://www.nist.gov/system/files/documents/2020/01/16/NIST-Privacy-Framework-Roadmap-v1.0.pdf>, p.4.

⁷⁵ Roadmap for Advancing the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise risk Management, January 16, 2020. Available at: <https://www.nist.gov/system/files/documents/2020/01/16/NIST-Privacy-Framework-Roadmap-v1.0.pdf>, p.4.

3.8.7 Priority area 7: Privacy workforce

According to NIST, currently the demand for a privacy workforce is outpacing the supply, while the benefits of adhering to the NIST Privacy Framework will be enhanced if there are more trained and educated privacy professionals.⁷⁶ The development of this workforce is a necessary prerequisite both to support organisations efforts in protecting people's privacy and to gain the benefits of the use of their data. The first step in creating this workforce is to come up with a common **taxonomy to categorise the privacy workforce**, for example privacy work roles, tasks and abilities.⁷⁷ In order to do so, the privacy workforce, education challenges and needs must be decided through discussions with stakeholders such as professional associations, academia and the public sector. Regarding outreach and mechanisms to develop a privacy and cybersecurity workforce coordination with the NIST National Initiative for Cybersecurity Education (NICE) program is also recommended.⁷⁸

3.8.8 Priority area 8: International and regulatory aspects, impacts and alignment

Lastly, NIST tackles the challenges created by globalization and interconnectedness of technology, including the need to comply with privacy requirements around the world.⁷⁹ The manifold requirements can not only impede interoperability and slow down innovation but may also have uncertain impacts on privacy. The fundamental obstacle for organizations is that they may be less inclined to operate internationally, since a complex privacy ecosystem may make them able to respond to new and evolving risks.

Consequently, the activities NIST acknowledges to address this issue focus on the engagement between NIST and governments, or entities in order **to familiarize them with the NIST Privacy Framework and, where possible, agree in approaches**.⁸⁰ Furthermore, it plans to work with industry stakeholders and support their global engagement. Finally, **information exchange** with standards development organizations, industry or sector players is a necessary component to ensure that the **Privacy Framework is aligned and compatible with existing or developing standards and practices**.⁸¹

⁷⁶ Roadmap for Advancing the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise risk Management, January 16, 2020. Available at: <https://www.nist.gov/system/files/documents/2020/01/16/NIST-Privacy-Framework-Roadmap-v1.0.pdf>, p.4.

⁷⁷ Roadmap for Advancing the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise risk Management, January 16, 2020. Available at: <https://www.nist.gov/system/files/documents/2020/01/16/NIST-Privacy-Framework-Roadmap-v1.0.pdf>, p.5.

⁷⁸ Roadmap for Advancing the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise risk Management, January 16, 2020. Available at: <https://www.nist.gov/system/files/documents/2020/01/16/NIST-Privacy-Framework-Roadmap-v1.0.pdf>, p.5.

⁷⁹ Roadmap for Advancing the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise risk Management, January 16, 2020. Available at: <https://www.nist.gov/system/files/documents/2020/01/16/NIST-Privacy-Framework-Roadmap-v1.0.pdf>, p.5.

⁸⁰ Roadmap for Advancing the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise risk Management, January 16, 2020. Available at: <https://www.nist.gov/system/files/documents/2020/01/16/NIST-Privacy-Framework-Roadmap-v1.0.pdf>, p.5.

⁸¹ Roadmap for Advancing the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise risk Management, January 16, 2020. Available at: <https://www.nist.gov/system/files/documents/2020/01/16/NIST-Privacy-Framework-Roadmap-v1.0.pdf>, p.5.

4 Evolving Landscape

4.1 European Regulatory Evolution Update

In the duration of the Cyberwatching.eu project, the regulatory landscape has evolved through a number of regulatory tools, including regulations, directives and manifold opinions, guidance, and tools aiming to guarantee a higher level of data protection to European citizens and an increased legal certainty.

4.1.1 General Data Protection Regulation (GDPR) and NIS Directive

The General Data Protection Regulation (GDPR) became the first landmark in the evolutionary landscape in Europe safeguarding data protection, transparency, purpose limitation, and many more rights and guarantees to data subjects.⁸² Following that, the Directive on security of network and information systems (NIS Directive) imposed a minimum standard on operators of essential services and digital services ensuring that the European critical infrastructure would be harmonized.

4.1.2 NIS2 Directive

The [updated Directive on Security of Network and Information Systems](#) – (NIS2 Directive) identifies how operators of essential services and providers of digital services will have to take security measures to ensure that their product remains secure, and reporting that will need to be done in the event of a security event. Also contains a recommendation for a risk assessment for supply chains.

4.1.3 ePrivacy Regulation

In brief, the ePrivacy Regulation⁸³ sets forth long term rules for how electronic communications must respect privacy of individuals data. It identifies areas in which new rules will apply and greater enforcement strategies.

The replacement of the ePrivacy Directive from the ePrivacy Regulation is currently the missing link in fortifying Europe's data protection efforts, through additional data protection rules for electronic communications providers and services of end-users. More details on the latest progress of the ePrivacy Regulation can be found in Deliverable D3.5 "Risk and Recommendations on Cybersecurity Services"⁸⁴, specifically Section 2.2 Updates on ePrivacy Regulation. It is expected that the new ePrivacy Regulation will tackle topics such as electronic direct marketing, and the use of cookies or other similar technologies.

4.1.4 AI Regulation

The relatively slow advancement in the ePrivacy Regulation, has not stopped the EU regulators from moving forward with a European legal framework to address fundamental rights and safety risks specific to AI systems (AI Regulation).⁸⁵ The AI Regulation aims to boost uncertainty in the industry players developing AI technologies, as well as to generate a framework which will ensure people's safety and fundamental

⁸² The History of the General Data Protection Regulation, available at: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

⁸³ About the ePrivacy Regulation available online at: <https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation>

⁸⁴ Cyberwatching.eu Deliverable D3.5 available online at: https://www.cyberwatching.eu/sites/default/files/D3.5_Risk_and_Recommendations_on_Cybersecurity_Services_v1.0_Final.pdf

⁸⁵ Regulatory framework proposal on Artificial Intelligence, the European Commission, available at: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>.

rights.⁸⁶ In addition to the AI Regulation, the Commission has proposed a 2021 review of the Coordinated Plan with Member States on Artificial Intelligence.⁸⁷ Furthermore, the Commission's AI Regulation proposal is part of package of three inter-related legal initiatives, including "EU rules to address liability issues related to new technologies, including AI systems", expected to be proposed on the last quarter 2021 or first quarter 2022, and the "Revision of sectoral safety legislation (e.g., Machinery Regulation, General Product Safety Directive), to be proposed on the second quarter 2021. The ability to engage in debates on the regulatory framework of emerging technologies such as Artificial Intelligence will offer a unique opportunity to all Cyberwatching.eu stakeholders to be actively involved in the possible global gold standard in AI regulation.⁸⁸ More concrete analysis of the legal changes and evolution of the AI sector can be found in D3.7 "White Paper around legal compliance and policy statements including recommendations".

4.2 Decision on the Cybersecurity Competence Centre in Bucharest

The decision to place the headquarters of the European Cybersecurity Competence Centre and Network (ECCC) in Bucharest was taken in 2020. And this represents an important step in putting the Cyber Security Act into operation. A number of preparatory activities are already being undertaken in parallel, including regular meetings of a "shadow" temporary governing board, which is for the time being preparing the path for the governing board that will be the effective control structure for the centre.

A full description of the centre and its make up⁸⁹ is contained below in the grey box, including details of its mission, task and organisation as a whole.

European Cybersecurity Competence Centre and Network

The European Cybersecurity Competence Centre (ECCC) aims to increase Europe's cybersecurity capacities and competitiveness, working together with a Network of National Coordination Centres (NCCs) to build a strong cybersecurity Community.

About ECCC

Mission

The **European Cybersecurity Competence Centre (ECCC)**, together with the **Network of National Coordination Centres (NCCs)**, is Europe's new framework to support innovation and industrial policy in cybersecurity. This ecosystem will strengthen the capacities of the cybersecurity technology Community, shield our economy and society from cyberattacks, maintain research excellence and reinforce the competitiveness of EU industry in this field.

The ECCC, which will be located in Bucharest, will develop and implement, with Member States, industry and the cybersecurity technology Community, a common agenda for technology development and for its wide deployment in areas of public interest and in businesses, in particular SMEs.

⁸⁶ A European approach to Artificial intelligence, the European Commission, available at: <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>.

⁸⁷ Coordinated Plan on Artificial Intelligence 2021 Review, the European Commission, available at: <https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review>.

⁸⁸ A European approach to Artificial intelligence, the European Commission, available at: <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence>.

⁸⁹ <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre>

The Centre and the Network together will enhance our **technological sovereignty through joint investment in strategic cybersecurity projects**.

Tasks

The Centre and the Network will make **strategic investment decisions and pool resources** from the EU, its Member States and, indirectly, the industry to improve and strengthen technology and industrial cybersecurity capacities, enhancing the EU's open strategic autonomy. The Centre will play a key role in delivering on the ambitious cybersecurity objectives of the [Digital Europe Programme](#) and [Horizon Europe](#) programmes.

The Centre together with the Network will support the deployment of innovative cybersecurity solutions. It will also facilitate collaboration and the sharing of expertise and capacities among all relevant stakeholders, in particular research and industrial communities, as well as public authorities, in the Community.

Regulation establishing the ECCC

On 8 June 2021, the Regulation establishing the European Cybersecurity Competence Centre and Network was published.

During the negotiations that led to the adoption of the Regulation, the EU co-legislators (the European Parliament and the Council) agreed in particular on a **co-financing approach** by which Member States commit to contributing to the work of the Centre and the Network, while keeping individual Member States' contributions voluntary.

The co-legislators also agreed on the distribution of **voting rights between Member States and the Union in the Centre's Governing Board**, giving the Union particular voting powers on decisions affecting the EU budget.

The ECCC is a new EU body established under articles 173(3) and 188(1) of the Treaty on the Functioning of the European Union (TFEU).

Organisation

The ECCC is currently being set up. The Commission will ensure the functioning of the ECCC until this new EU body can operate autonomously.

The ECCC administrative and governance structure includes:

- A **Governing Board** which provides strategic orientation and oversees ECCC activities.
- An **Executive Director** who is the ECCC's legal representative and is responsible for its day-to-day management.
- A **Strategic Advisory Group** that ensures a comprehensive, ongoing and permanent dialogue between the Community and the Competence Centre.

The ECCC will closely cooperate with the **Network of National Coordination Centres (NCCs)**, one per Member State, which support the cybersecurity Community at national level and under certain conditions can pass on EU funding.

Composition and operation of the Governing Board

Members of the Governing Board: One representative from each Member State and two representatives from the Commission (and an alternate for each representative), with cybersecurity knowledge and managerial skills; **renewable term of four years**

Observers, including ENISA as permanent observer, and other observers on an ad-hoc basis

A **Chairperson and a Deputy Chairperson** elected among the members of the Governing Board for three years, once renewable.

The **Executive Director** will take part in the meetings of the Governing Board but shall have no right to vote.

Decision making

In principle, **all decisions are taken by consensus** among the members of the Governing Board.

Where decisions cannot be taken by consensus, decisions shall be taken by a **majority of at least 75%** of all votes, with every Member State and the Commission having one vote. For decisions concerning the description of “joint actions” and the conditions of their implementation, the vote is proportional to the financial contributions of the members participating in the action.

The Union holds 26% voting rights for decisions affecting the EU budget.

Key functions of the Governing Board

- To provide **strategic orientations and oversee the Centre’s activities**
- To adopt the **work programme, annual budget, consolidated annual activity report**
- To adopt the **financial rules, the anti-fraud strategy, rules for the prevention and management of conflicts of interest, communication policy**
- To set up **working groups within the Community**
- To appoint the Executive Director and the Accounting Officer
- To appoint the members of the Strategic Advisory Group

Executive Director

- Responsible for the **day-to-day management** of the Centre
- Responsible for the **implementation** of the tasks assigned to the Centre by the Regulation
- **Assists and supports the Governing Board** on behalf of the staff of the ECCC
- Prepares and implements the work programme and **reports to the Governing Board**

National Coordination Centres (NCCs)

- One NCC from each Member State
- **Nominated by Member States** and notified to the Commission
- Possess or have access to research and technological expertise in cybersecurity
- Key function: **national capacity building**, and link with existing initiatives and national cyber community
- Can effectively **engage and coordinate** with industry, academia and research community, citizens, and the public sector and authorities under NIS
- **Can receive direct EU grants**
- Can provide **financial support** to third parties

Strategic Advisory Group

- **Composition: 20 members** appointed by the Governing Board from among the representatives of the entities of the cyber Community
- **Expertise** in cybersecurity research, industrial development, professional services or products
- Two-year term, once renewable
- Meets at least three times per year

Tasks:

- Advises the Governing Board on establishing working groups
- Organises public consultations to collect input that it provides to the Executive Director and the Governing Board with regard to the agenda, the annual work programme and the multi-annual work programme

cyberwatching.eu partners plan to disseminate the EU Project radar to the Competence Centre for potential use by them.

4.3 Evolution of ECSO (2.0 and 3.0)

With the creation of the European Cybersecurity Competence Centre and Network there is an obvious evolution of the European Cyber Security Organisation (ECSO) in order to ensure that the key stakeholders needs and requirements are being addressed within these new structures.

In the current model, ECSO includes: public sector, academic, research, large industry, SMEs, associations, and users as members – however, with the new competence centre, the public administrations will have a direct role and as such the requirement for their continuing membership within ECSO will not be absolutely necessary. And the role of the ECSO NAPAC will be replaced by the governing board role for the EU Member states within the competence centre structure.

A number of different models for the evolution of ECSO to ECSO 2.0 and even ECSO 3.0 have already be proposed, but it would be premature to define the exact path.

Suffice it to say that ECSO does truly represent the cybersecurity community as a whole and as such will have a primary and similar role within the new structure of the competence centre.

It could be envisaged that ECSO 2.0 or 3.0 may have two parts: 1) one part which is dedicated to market and financial aspects (business side), and 2) one part which is focused upon research and development and policy. Thus, it is possible that the organisation can fulfil more than one role in its future incarnation. As described in the next section, the development of the cyberwatching.eu Marketplace and re-packaging as the ECSO SME Registry will therefore play an important role for the business side.

The most logical cybersecurity “community” structure would be the combination and integration of the 4 large cybersecurity competence network pilot projects (CyberSec4Europe, CONCORDIA, ECHO and SPARTA) with ECSO to form a “mega” community cybersecurity ecosystem across Europe.

Given ECSO’s current working groups, it could be envisaged that each would have its role as well in the future structure, taking and combining as well all of the best parts of the 4 pilots focus groups and the outputs and work of the pilot projects.

Furthermore, as there appears a draft CSA topic in the Digital Europe Programme for funding the operation of this network and community, the financial base would be in place for the future of the organisation (if successful in obtaining the funding via the DEP proposal process).

4.4 Horizon Europe Programme and Digital Europe Programme

4.4.1 Horizon Europe Programme

Horizon 2020 was born to support the implementation of the “Europe 2020” Strategy and the “Innovation Union” flagship initiative and has contributed to addressing the main challenges of society, creating and maintaining industrial leadership in Europe and reinforcing scientific excellence, essential for sustainability, prosperity and the long-term well-being of Europe. In the field of **cybersecurity**, Horizon 2020 has made

available different localized financing lines, mainly in the programs: “Secure Societies” (Social Challenge 7); in “Information and Communication Technologies” (LEIT-ICT) and in “Health, Demographic Change and Well-being” (Social Challenge 1).

The new Framework Program for R & D of the European Union will be operational during the period 2021-2027. **Horizon Europe** will finance R + D + i projects in cybersecurity through the **Cluster 3 program "Civil Security for Society"**. This cluster responds to the challenges arising from persistent security threats, including cybercrime, as well as natural and man-made disasters.

Over the next seven years, the European Commission plans to mobilize **€ 1.596 billion** in funding for cybersecurity through this programme.

EU civil security research is one of the building blocks of the Security Union. Research in cluster 3 supports the following policies:

- fighting crime and terrorism (including organised crime and cybercrime)
- border management (including customs security and maritime security)
- resilient infrastructure
- cybersecurity (including security of network and information systems and certification)
- disaster-resilient societies (including against chemical, biological, radiological and nuclear (CBRN) incidents; climate-related risks and extreme events; geological disasters, such as earthquakes, volcanic eruptions and tsunamis; pandemics)

The first work programme 2021-2022 for cluster 3 was expected in mid-June 2021, and it will finance R & D & I projects related to cybersecurity for an amount of around € 140 million.

- Specifically, projects will be financed in the following lines:
- Resilience of interconnected systems and digital infrastructures.
- Certification and quantification.
- Security of the supply chain.
- Advanced cryptography.
- Artificial intelligence to reinforce cybersecurity.
- Tools that guarantee the security and privacy of personal data.

4.4.2 Digital Europe Programme

The general objectives of the Digital Europe Programme (DEP) shall be to support and accelerate the digital transformation of the European economy, industry and society, to bring its benefits to citizens, public administrations and businesses across the Union, and to improve the competitiveness of Europe in the global digital economy while contributing to bridging the digital divide across the Union and reinforcing the Union’s strategic autonomy, through holistic, cross-sectoral and cross-border support and a stronger Union contribution.

DEP has five interrelated specific objectives:

- High Performance Computing
- Artificial Intelligence
- Cybersecurity and Trust
- Advanced Digital Skills
- Deployment and Best Use of Digital Capacity and Interoperability

The financial contribution from the Union under **Specific Objective 3 – Cybersecurity and Trust** shall pursue the following operational objectives:

- support the building-up and procurement of advanced cybersecurity equipment, tools and data infrastructures, together with Member States, in order to achieve a high

- common level of cybersecurity at European level, in full compliance with data protection legislation and fundamental rights, while ensuring the strategic autonomy of the Union;
- support the building-up and best use of European knowledge, capacity and skills related to cybersecurity and the sharing and mainstreaming of best practices;
 - ensure a wide deployment of effective state-of-the-art cybersecurity solutions across the European economy, paying special attention to public authorities and SMEs;
 - reinforce capabilities within Member States and private sector to help them comply with Directive (EU) 2016/1148 of the European Parliament and of the Council including through measures supporting the uptake of cybersecurity best practices;
 - improve resilience against cyberattacks, contribute towards increasing risk-awareness and knowledge of cybersecurity processes, support public and private organisations in achieving basics levels of cybersecurity, for example by deploying end-to-end encryption of data and software updates;
 - enhance cooperation between the civil and defence spheres with regard to dual-use projects, services, competences and applications in cybersecurity, in accordance with a Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (the 'Cybersecurity Competence Centre Regulation').

Over the next seven years, the European Commission plans to mobilize **€ 1.650 million** in funding for cybersecurity through this programme. The actions under Specific Objective 3 shall be implemented primarily through the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres in accordance with the Cybersecurity Competence Centre Regulation.

5 Conclusions and Recommendations

5.1 Common denominators



Figure 5-1: Key Priorities Importance Graph

It is both relevant and important to note the common areas and common threads appear not only in cyberwatching.eu research, but also can be found throughout the roadmaps that we have studied and analysed in this deliverable. These include, but are not limited to the following:

1. Trust and Accountability addressing the issue of confidence in which products, solutions and service that you use
2. Governance with respect to harmonisation, compliance, national application of regulations issues
3. Data Security and Privacy as this relates to the General Data Protection Regulation, while at the same time there is an urgent need for tools and guidance on compliance aspects
4. Education, Training and Awareness involving all of the specialised skillset to increase capabilities, capacity and expertise in cybersecurity, certification and standards especially - also with the goal of addressing the significant challenge of retaining expertise in Europe
5. European and International Cyber Security Certification filling the gaps and striving to keep up with the evolution and expansion of emerging technologies
6. Cross-border business requirements which were highlighted as a specific issue and challenge during the COVID pandemic
7. SMEs lack the resources and support tools and require training as well as their issue of retaining trained Human Resources
8. Cybersecurity standards have issues related to cost, the understanding of experts in the field and new standards within the context of new and changing technologies
9. Resilience represents an important issue for critical infrastructure as well as the economic and social fabric of society
10. The lack of an Ethics Code of Conduct as a result of changing, new and emerging technologies

All of these aspects are common to the cyberwatching.eu research and the roadmaps studied and as such represent important points to be addressed in the future.

5.2 Cyberwatching.eu Project

Cyberwatching.eu has already had a significant impact upon the cybersecurity community and European cybersecurity as a whole with clear elements from the project which will continue not only to exist, but also to thrive well after the end of the project and the project funding.

Cyberwatching.eu has gathered recommendations across its work packages, stakeholder community and has summarized the recommendations in Table 2-2 to Table 2-6.

This impact is the clear legacy of the Cyberwatching.eu project and this has laid the basis for a number of tools which make the life of cybersecurity concerned policy makers, research project consortia and SMEs much easier. These tools are mentioned hereafter.

5.2.1 Project Radar

The EU Project Radar provides information which can users understand the CS&P R&I landscape. It provides a high-level visualization of funded projects organized by high-level categories, their lifecycle stage and relative market and technology maturity. It can also be used to zoom in on technology and vertical sectors (defined by the JRC cybersecurity taxonomy) in order to identify projects that are focusing on these areas.

The Radar's primary value proposition is that of saving the user time and money by processing and analysing detailed landscape data for the user. It allows the user to make swift yet statistically sound statements on the state of the art of the European cybersecurity and privacy research landscape. Generic in its implementation, the Technology Radar technology can be adapted to other domains with reasonable effort, making it a valuable asset in the toolbox for anyone seeking oversight of an inherently complex landscape.

Transformed since 2017 from a static report into what is now a live, autonomous online resource which is fully integrated into the cyberwatching.eu website and managed by registered users (representatives from the projects). The radar links to the project hub meaning that users can access mini-sites, also managed by projects, to find out more information including current activities and results, as well as directly contact them.

The Radar mainly targets policymakers, the research community, and as is reported in D5.3 is of interest to SMEs. The radar however, is only as relevant as the data it shows. Therefore, the live version must be continuously updated requiring direct engagement with the R&I community. To do this, Trust-IT and UOXF are committed to sustain the radar beyond the project lifetime. We are particularly interested in continuing dialogue with the EC, JRC and the newly defined Competence Centre to see how the radar could be further sustained in the long-term and included in for example the Cybersecurity Atlas.

The radar has been a continuous priority since day one of the cyberwatching.eu project and strong focus of our previous Project Officer Nineta Polemi and our reviewers.

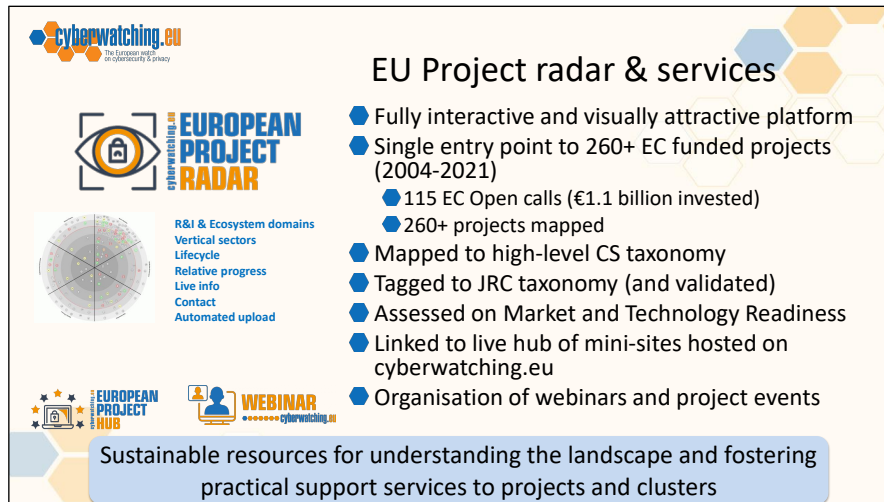


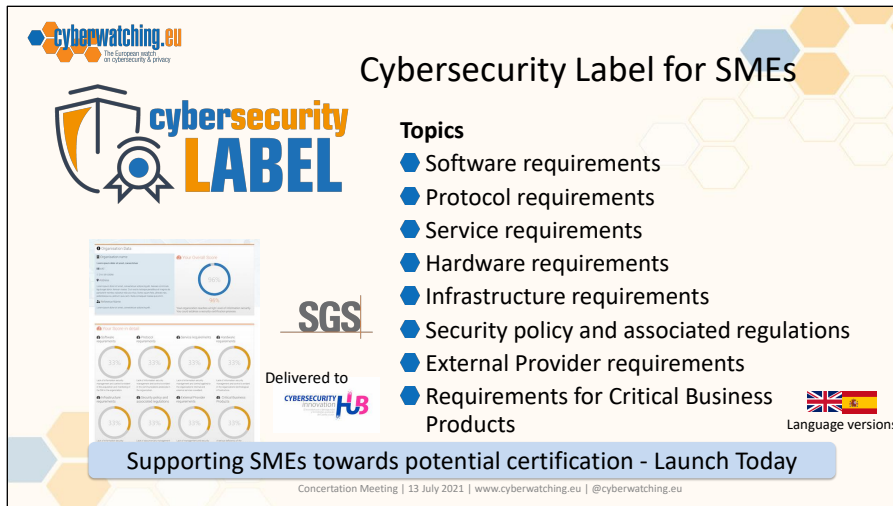
Figure 5-2: EU Project Radar and Services

Built on a sound MTRL methodology⁹⁰, the MTRL self-assessment resource which is integrated into the EU Project Radar, is a way for projects to evaluate their evolution, not only in relation to the technology, but also in relation to the market. It has also been an instrument for projects collaboration (like joint webinars= based on to their Market Readiness in a specific time. It should be a good practice for projects to do intermediate self-evaluations, beyond the mandatory reviews with the EC, to check that their project is progressing correctly at the technological and market level, and more specifically, comparing to the relative performance of other projects in the same cybersecurity domain. The successful webinar series is also a key asset of the project and will be sustained beyond the project lifetime as a paid service. The services leverage the EC's strategy to encourage projects to cluster for dissemination activities in order to increase impact and reach of project results.

5.2.2 Light Cybersecurity Assessment and Label

Certification is the key to fighting the defragmentation of the cybersecurity market in Europe, but for SMEs it represents an investment of time and money that they cannot always afford. The development of a **light cybersecurity label** so that SMEs can identify their areas of improvement in cybersecurity and allow them to apply the first corrective measures, is a prior and necessary step towards the certification process. The objective of the **light cybersecurity label** will be to act as a gateway for SMEs to the certification process, for which it will be promoted through the Cybersecurity Innovation Hub (CyberDIH) coordinated by the AEI de Ciberseguridad, whose ultimate purpose is to help SMEs in their digital transformation processes. Through the European Network of Digital Innovation Hubs, the **light cybersecurity label** will be made available to all European SMEs that require it, considering the possibility of establishing collaboration agreements with other EDIHs for its promotion.

⁹⁰ <https://cyberwatching.eu/d23-methodology-classification-projects-services-and-market-readiness>



The slide features the Cyberwatching.eu logo at the top left, with the tagline 'The European expert on cybersecurity & privacy'. The main title is 'Cybersecurity Label for SMEs'. Below the title is a shield icon with a magnifying glass and the text 'cybersecurity LABEL'. To the right, a list of topics is shown with blue hexagonal bullet points. In the center, there is a screenshot of a dashboard with various charts and the SGS logo. Below the screenshot, it says 'Delivered to CYBERSECURITY INNOVATION HUB'. At the bottom, there is a blue banner with the text 'Supporting SMEs towards potential certification - Launch Today' and a footer with 'Concertation Meeting | 13 July 2021 | www.cyberwatching.eu | @cyberwatching.eu'. On the right side, there are flags for the UK and Spain with the text 'Language versions'.

Cybersecurity Label for SMEs

Topics

- Software requirements
- Protocol requirements
- Service requirements
- Hardware requirements
- Infrastructure requirements
- Security policy and associated regulations
- External Provider requirements
- Requirements for Critical Business Products

Delivered to
CYBERSECURITY INNOVATION HUB

Supporting SMEs towards potential certification - Launch Today

Concertation Meeting | 13 July 2021 | www.cyberwatching.eu | @cyberwatching.eu

Language versions

Figure 5-3: Cyberwatching.eu Cybersecurity Label for SMEs

5.2.3 The GDPR Temperature Tool and Information Notice Tool

The GDPR tool is an online self-assessment questionnaire targeting SMEs to facilitate their understanding of where they stand with respect to the GDPR in terms of “risks to sanctions”. By answering each question, the points towards their “Risk of Sanction Level” can increase or decrease. At the end, the respondent receives a valuable report of the recommendations for each question answered, as well as a total “temperature” (green, yellow or red) representing the respondent’s risk of sanction level (low, medium, high, or very high).

The tool has been enhanced with the 2.0 version, which updated the recommendations with the latest legal best practices, and introduced new features such as the integration of solutions and tools from the cyberwatching.eu marketplace and a “further reading” section. The value of this tool is that it collects many available opinions, guidance and tools – therefore on the one hand acting a repository of knowledge to the SMEs’ availability – and on the other hand distributes other online tools, solutions and software that can improve their compliance.

The Information Notice Tool has been created to help organisations have a more robust GDPR posture. The tool provides a practical check-list for the components required in an Information Notice under the GDPR. This includes all the elements required for an Information Notice based on a set of questions related to data processing by any type of company, providing useful recommendations on how to comply with the GDPR rules. Users receive a downloadable report which includes the recommendations tailored to their responses.

Both tools will be promoted through the Cybersecurity Innovation Hub (CyberDIH).

GDPR resources for SMEs

- Understand risk exposure to sanctions
 - Individual consent for data processing
 - Services to children aged 13 or over
 - Automated processing of personal data
 - Data transfer out of EU...
 - Version 2.0 – July 2021
- Practical check-list for the components required in an Information Notice under the GDPR

GDPR sanctions can impact greatly on any organisation

Figure 5-4: GDPR Temperature Tool

5.2.4 Risk Assessment Tool

AON have created a Cyber Risk Assessment Tool for SMEs that allows companies to gain understanding of the potential cyber risks their company faces. It takes the form of a two-part questionnaire: the first part asks for a personal assessment of the company’s IT security, while the second part is more focused on the technical aspects of the company’s IT security and the cybersecurity strategy (if one is available). Based on the answers, the company is then assigned a profile according to the level of vulnerability and receive a preliminary risk assessment.

The tool will be promoted through the Cybersecurity Innovation Hub (CyberDIH).

Risk Management guidance for SMEs

Topics

- Capacity building
- Cybersecurity framework
- Who has admin rights to company systems
- Acceptable use and access authorisation policies
- Log in authentication
- Regularity of password changes
- Regularity of vulnerability assessment and remediation plan for systems
- Intrusion detection system
- Regularity of back-up

A lightweight way to understand areas at risk

Figure 5-5: Risk Assessment Tool for SMEs

5.2.5 The ECSO SME Hub - Built upon the cyberwatching.eu marketplace core “engine”

The marketplace is a unique platform which showcases both CS&P results from R&I projects in a market-oriented way and together with services and products from European SMEs. “Products” are categorised according to the NIST cybersecurity framework to facilitate user experience and interaction. Therefore, projects transition from the EU Project Radar and project Hub from R&I activities, where we focus on their R&I activities and classify them by R&I taxonomies (cyberwatching.eu taxonomy

and JRC taxonomy); to the marketplace where rather the focus and information is about actual results which are classified by the NIST cybersecurity taxonomy.

The dynamic nature of the tailor-made marketplace match many of the specs for the ECSO SME Registry. New functionalities have been added including new user types, jobs corner, payment modules, fields relating to standardisation and integration of an already established SME database of 500 companies to meet ECSO needs. The marketplace will be handed over to ECSO at the project end and it will become the SME Registry, sustained in the future by them. This will be a central asset for ECSO in terms of its mission to provide support to building trust in cybersecurity solutions and best practices in Europe.



Figure 5-6: Cyberwatching.eu Marketplace > ECSO

5.2.6 SMEs – Overall Recommendations for The Future

SMEs have a vital role to play in the development of Europe’s cybersecurity capacities, and roadmaps and long-term goals should reflect this. From ensuring that support is available so that new products and services are built secure, to sharing threat intelligence so that companies remain secure and products and services can be developed to counter them, a range of considerations need to be made so that Europe can leverage its strong SME base. Actions such as these, and developing based upon existing European technologies and capacities, will mean that the agility of European companies and SMEs will be able to take products and services and offer them across a range of vertical services, ensuring European digital sovereignty and the long term cyber security of Europe.

5.2.7 Regulatory Landscape

In conclusion, whilst the future of the regulatory landscape may seem uncertain or lengthy due to its complexity, but the near future will facilitate organizations’ efforts in complying with data protection and privacy regulations.

The legal certainty will be enhanced by clarifying and creating more specific requirements on data protection through the upcoming ePrivacy Regulation and AI Regulation. This progress will, in hand, also create the need for higher stakeholder engagement, in order to ensure that the stakeholders have all the necessary tools to comply with their new obligations.

5.2.8 R&D Landscape

The continuous analysis of the EC-funded R&D projects has allowed cyberwatching.eu and the EC to have an almost real-time vision of the cybersecurity priorities covered and those that remain to be covered, which allows redirecting the investments in R&D to fill the gaps. We recommend the EC encourage projects to register and join the Project Radar and periodically complete an MTRL analysis in order to allow better use of the results of the projects and plan concrete actions from EC to minimize barriers to the commercialization of solutions within the priorities that have a low market maturity.

A key recommendation from Deliverable D2.7 is that it is clear with the time-based progression through the radar that without new projects coming on board, being analysed for inclusion in the project hub and then included in the radar that the radar as a tool will start to become less and less useful. We would therefore recommend to the Commission that there should be a strategy for the continuation of tools such as this that require small but consistent support to ensure that the initial investment continues to be useful in generating a return. This will be of particular importance with the new Horizon Europe calls and hence new projects join the cybersecurity ecosystem and themselves need to understand their progress and the possible routes to exploitation of their outputs.

5.3 Four Pilots & ECSO Cybersecurity Research Focus Areas Priorities

The Four Pilots and ECSO Roadmapping Focus Group has summarized the cybersecurity research focus area priorities below:

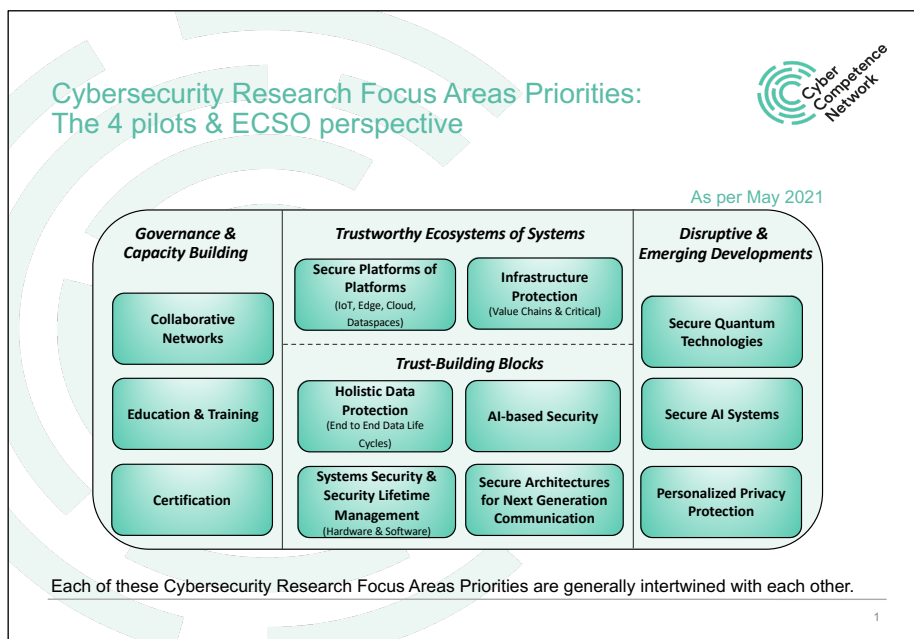


Figure 5-7: 4 Pilots & ECSO Perspective of Focus Area Priorities for Cybersecurity Research

It is clear that although the approaches toward the future roadmap are different in looking at the 4 pilots and ECSO, a number of key elements continuously appear in all and have a certain importance. The key to the future continues to be the collaboration and the expansion and integration of the network of the Cybersecurity Community ecosystems with the European Cyber Security Competence Centre (Bucharest) at the centre and having key nodes and networks emanating and connected to ECSO and the 4 pilot projects. Furthermore, the national cyber security competence network is a key element in this grand scheme. This is significant for the protection and security of

the European citizen and society with respect to Cybersecurity and the economic future of Europe. The key areas addressed in each of the roadmaps and forward-looking efforts are complementary in nature while ensuring that all of the important aspects are comprehensively covered. This deliverable represents the culmination of the work effort of the cyberwatching.eu project and is the first time that all of the roadmaps have been summarised with snapshots for the benefit of all of the key stakeholders (starting with the European Institutions, the EU Member States Public Sector, the European Cybersecurity Community and the European Cybersecurity Ecosystem).

ANNEX A. GLOSSARY

Term	Explanation
AAA	Authentication, Authorization and Accounting
AGID	Agency for Digital Italy
AI	Artificial Intelligence
AIRE	Atos Incident Reporting Engine
AML	Anti-Money Laundering
AUP	Acceptable Use Policy
B2B	Business-to-Business
B2C	Business-to-Consumer
CAPE	Continuous Assessment in Polymorphous Environments
CDX	Cyber Defence Exercises
CEN	Comité Européen de Normalisation
CENELEC	European Committee for Electrotechnical Standardization
CONCORDIA	Cybersecurity cOMpteNCe fOr Research and InnovAtion
COTS	Commercial Off-The-Shelf
CPS	Cyber-Physical Systems
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
CyberSec4Europe	Cyber Security for Europe
DEP	Digital Europe Programme
DLT	Distributed Ledger Technologies
DPIA	Data Protection Impact Assessments
EAP	Extensible Authentication Protocol
EBA	European Banking Authority
ECCE	European Cybersecurity Competence Centre and Network
ECHO	European network of Cybersecurity centres and competence Hub for innovation and Operations
ECSSO	European Cyber Security Organisation
E-FCR	ECHO Federated Cyber Range
ETSI	European Telecommunications Standards Institution
ENISA	European Agency for Network and Information Security

Term	Explanation
ETSI	European Telecommunications Standards Institute
E-EWS	ECHO Early Warning System
FATCA	Foreign Account Tax Compliance Act
FIDO	Fast Identity Online
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite Systems
HAIIT	High-assurance Intelligent infrastructure toolkit
ICS	Information and Communication Systems
IDS	Intrusion Detection Systems
II	Intelligent Infrastructure
JRC	Joint Research Centre
KYC	Know Your Customer
LCL	Lightweight Cybersecurity Label
LEO	Low Earth Orbit
MISP	Malware Information Sharing Platform
MTRL	Market & Technology Readiness Level
NIST	National Institute of Standards and Technology
NLP	Natural Language Processing
NSB	National Standardisation Bodies
PET	Pet Enhancing Technologies
PSD2	Payments Service Directive 2
PSIRT	Product Security Incident Response Team
QKD	Quantum Key Distribution
RASP	Runtime Application Self Protection
R&I	Research and Innovation
SCA	Strong Customer Authentication
SMPC	Secure MultiParty Computation
SPARTA	Strategic programs for advanced research and technology in Europe
SRIA	Security Research and Innovation Agenda
SWOT	Strengths, Weaknesses, Opportunities, and Threats

Term	Explanation
TATIS	Trustworthy APIs for enhanced Threat Intelligence Sharing
TIE	Threat Intelligence Integrator
TG	Threat Group
UAVS	Unmanned Aerial Vehicles System
V2I	Vehicle-to-Infrastructre
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VA	Vulnerability assessment
VNSF	Virtual Network Security Functions
xAI	Explainable Artificial Intelligence