SPARTA

D3.5

SPARTA SRIA

Lessons Learned and Future Assessment

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

Deliverable type	Report
Deliverable reference number	SU-ICT-03-830892 / D3.5 / V1.0
Work package contributing to the deliverable	WP3
Due date	March 2022 – M38
Actual submission date	24th May, 2022

Responsible organisation	TUM
Editor	Marius Momeu
Dissemination level	PU
Revision	V1.0

Abstract	Software and hardware have become ubiquitous in the modern European society thus rendering IT security as a central topic for establishing and maintaining digital sovereignty in the EU. As such, the SPARTA network developed a strategic research and innovation agenda throughout its lifetime, which proposes a mid- to long-term vision on cybersecurity research for strengthening EU's digital sovereignty. In this deliverable, we first describe our findings from SPARTA's roadmapping process, and then propose recommendations for future roadmapping exercises.
Keywords	Roadmap, Lessons learned, Future assessment

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

Editor

Marius Momeu (TUM)

Contributors (ordered according to beneficiary numbers)

Marius Momeu, Claudia Eckert (TUM)

Thomas Jensen (INRIA)

Artsiom Yautsiukhin, Fabio Martinelli (CNR)

Reviewers (ordered according to beneficiary numbers)

Jan Hajny (BUT)

Vincent Thouvenot (TCS)

Executive Summary

This document summarizes the lessons learned during the process of establishing and maintaining a strategic research and innovation roadmap in SPARTA. Based on these findings, this document gives recommendations that further cybersecurity roadmapping exercises in the EU could benefit from.

The SPARTA roadmap has been maintained as a living document throughout the lifetime of the project, incrementally developed in an agile and open fashion with ongoing input from the SPARTA network of partners, associates, and friends. The vision and the milestones of the roadmap were built around the clearly defined ambitious mission of strengthening EU's digital sovereignty. Nevertheless, the roadmap outlines several specific challenges that need to be addressed in order to achieve its overarching mission, which, in turn, require sub-challenges of their own.

The focus of the SPARTA roadmap was on identifying technological challenges required for achieving digital sovereignty, analysed from the perspectives of research, education, and certification. The final release of the roadmap has been developed over 36 months throughout the SPARTA project, accounting for 4 deliverables, each representing an enhanced version of the previous one.

This is the 5th and final deliverable of WP3, built around learnings from developing the 4 roadmap versions. Specifically, the document starts with an introduction in Chapter 1 that describes several roadmapping activities carried in SPARTA emphasizing the lessons learned while implementing them. The document then proceeds with Chapter 2 where we outline several recommendations for roadmapping processes, based on the lessons learned described in the previous chapter.

Table of Content

Chapter 1 Lessons Learned in SPARTA

Roadmapping

The overarching goal of the SPARTA roadmap is to provide mission-driven and strategic guidance to European decision-makers and the European Commission for defining future projects and investments in cybersecurity. Specifically, the SPARTA roadmap aims to close the technology as well as cybersecurity-skill gap in the EU and to outline new and emerging challenges in cybersecurity with respect to research, education, and certification. These objectives ought to assist in developing a mid- to long-term vision to strengthen Europe's cybersecurity capabilities, aligned with EC's strategy for Horizon Europe, Digital Europe, and other similar funding programmes.

1.1 Roadmap Mission

Throughout its lifetime, the SPARTA network was guided by one, clearly-stated ambitious mission: strengthening Europe's digital sovereignty. Digital sovereignty has emerged as a central objective within the EU, seeking to empower the greater EU-wide goal of achieving strategic autonomy. This initiative was motivated by several observations:

- EU citizens and industries should be able to control and protect their personal data, in a digital environment where most cloud infrastructures are managed by non-EU providers.
- EU industries should remain at the forefront of innovation in the IT sector.
- IT products and services used throughout the EU should be certifiable, in accordance with key EU values such as trust and transparency.
- The COVID-19 pandemic that started in 2020 has further contributed to demonstrate how dependable society is on reliable and secure digital infrastructures.

As such, the SPARTA roadmap choses to analyze the scientific and technological cybersecurity challenges that must be met in order to strengthen EU's digital sovereignty and to construct a secure and trustworthy digital single market across the Member States.

The SPARTA roadmap was established and maintained through a hybrid bottom-up and top-down approach. On one hand, SPARTA's overarching mission of strengthening digital sovereignty and the overall scientific challenges required to achieve it (e.g., trustworthy software and hardware, user-centric data governance, secure artificial intelligence) were defined in a top-down manner by a central committee of roadmap stakeholders. On the other hand, the more concrete steps and timelines to solve these challenges were highly based on input from the whole network in a bottom-up fashion (e.g. the technological, education, and certification sub-tasks that are defined for each roadmap challenge).

On par with contemporary software and hardware, cybersecurity is ubiquitous and can thus impact several industries that Europeans rely on, such as medical, transportation, supply chain & manufacturing, or critical infrastructures, just to name a few. However, there is no "one size fits all" in cybersecurity. Setting one clearly-defined ambitious mission to build roadmap challenges around was a highly beneficial trait in SPARTA. It represented a concrete goal that drives prioritizing challenges for the roadmap, which facilitated productive roadmapping exercises focused on achieving concrete milestones. As such, the sub-challenges defined in a bottom-up fashion were given the required details to match the top-down objectives. Moreover, as SPARTA's mission of strengthening digital sovereignty is shared across the EU, it enabled us to find overlapping and complementary aspects in similar roadmapping initiatives aligned with SPARTA, such as the agendas built by the other pilot projects and ECSO.

1.2 Analysis on Existing Roadmaps

In order to get a holistic view of the cybersecurity vision within the EU, we have carried an analysis at the beginning of SPARTA on national and EU-international cybersecurity roadmaps. Our findings including the analysed roadmaps are described in Chapter 3 of the SPARTA roadmap[1]. This exercise facilitated the process of identifying cybersecurity topics that have already received increased attention on the one hand, and challenges that were not in focus on the other hand. In total we have analysed 18 national roadmap and strategy documents, aiming to take visions of different EU Member states (11 in total) fairly (e.g., without excessive reliance on documents provided by one (of a few) Member state(s) only). Also, seven EU-international cybersecurity roadmaps produced by different initiatives, organisations and projects were analysed separately.

Once we curated the documents with cybersecurity agendas, we extracted the challenges addressed and mapped them onto the JRC's three-dimensional taxonomy[2]. We deemed the JRC taxonomy a comprehensive-enough scheme, as it intertwines three dimensions of high relevance for classifying challenges in cybersecurity research and innovation: a) research domains (s.a., Data Security and Privacy or Network and Distributed Systems), b) applications and technologies (s.a. Artificial intelligence or Quantum Technologies), and c) sectors (s.a. Health and Transportation). This analysis helped us to 1) confirm that the directions selected by SPARTA (and its 4 scientific programs) are of high importance; 2) focus on elaborating the top priorities; and 3) ensuring that SPARTA's roadmap does not miss important directions.

Analysing the documents, we identified the issues explicitly mentioned in the documents and then counted the number of documents referencing every issue. The issues with top count are considered the most influencing, since more documents dedicate explicit attention to them.

We would like to note that our analysis was focussed on identifying the top priorities, rather than on ranking all possible topics. For example, cybersecurity challenges that were considered of only moderate importance received a very low (sometimes 0) score in our analysis. *This should by no means be treated as the topic is of no importance at all*. In addition, our analysis was performed on documents targeting civil research, which explains the low score for important applications of cybersecurity technologies, such as defence. National roadmaps, on the contrary, often underline the need to increase cyber security preparedness of their defence forces. Because of the misalignment in the nature of the analysed documents on this topic, we do not focus on this issue, even though we agree that cyber defence is one of the top domains for cyber security.

The validity of the results highly depends on the quality of the curated documents. These documents were provided by national partners from SPARTA, as it was assumed they have good knowledge about the cybersecurity R&I landscape in their countries, since they play a significant role in shaping it. Furthermore, the SPARTA partners have participated in numerous European roadmap activities (e.g., projects, various committees, European organizations) and have good knowledge of the key documents influencing European research funding programs (e.g., Horizon 2020). Thus, we were confident that the partners within SPARTA have excellent expertise and are heterogeneous enough to select the best set of materials for the analysis.

Although the analysed EU roadmaps are older than a number of national cyber security strategies we considered the trends identified by the latter coincide well with those addressed by the former. In other words, many trends which are acknowledged by national authorities now, have been predicted by EU roadmaps several years before. SPARTA's roadmap aims for having similar (and, maybe, an even more long-lasting) effect.

We also see that by analysing national strategies it is possible to identify the main trends in cyber security (although, with a slight delay), but with a focus on national-level priorities, like raising

[1] Deliverable D3.4: *Updated SPARTA SRIA (Roadmap v3)*, PU, M36
[2] http://publications.jrc.ec.europa.eu/repository/bitstream/JRC118089/taxonomy-v2.pdf

awareness, raising cyber skill level of the law enforcement agencies, work on cyber security standards and fostering compliance, etc. Such analysis should be taken with a pinch of salt, as many important, but more technical topics (such as cryptography) or foundational topics (such as formal models) are too technical for the documents of this level. Nevertheless, is it clear that governments start dedicating significantly more attention to cyber security.

1.3 Agile Roadmap Design

Considering the ever-evolving nature of cybersecurity, SPARTA's roadmapping process was designed to be *agile*. Starting with a roadmap nucleus the SPARTA roadmap was updated and systematically extended in an annual cycle. This enabled us to address emerging trends and issues in early stages. In addition, the roadmapping process was designed to be *open*, thus facilitating partners and associates from the consortium to have a say in the developments of the roadmap.

The annual roadmap update followed an iterative process. The SPARTA's Roadmap Committee led the evolution of the roadmap by initiating discussions for stimulating roadmap contributions, by coordinating exercises and workshops for collecting input on the roadmap, and by updating the roadmap by reviewing and integrating the received contributions. Broadly speaking, a roadmap iteration involved the following sequence of steps:

1. Internal brainstorming initiated and coordinated by the Roadmap Committee within the SPARTA network of scientific programmes and challenges.
2. Additional discussions with associates and friends in dedicated workshops (described below).
3. Consolidating and synthesizing all received input, and integrating it into previous release.
4. Aligning and synchronizing the roadmap process and results with the other CCN pilots and ECSO.

Thus, throughout its lifetime, the SPARTA roadmap was maintained as a living document, updated periodically while taking into consideration the latest technical, educational, and societal developments, as well as the identification of emerging issues. Furthermore, each of the existing SPARTA challenge pinpoints its own program-specific roadmap with defined sub-goals in terms of research, education and certification, and a timeframe towards their successful completion. The roadmap challenges are thoroughly described by Chapters 6-8 of the SPARTA roadmap[3].

The agile and open roadmapping process generally proved to be very productive in SPARTA. The initial roadmap challenges, introduced in the first roadmap release[4], were defined on the basis of 60 seed challenges, proposed by SPARTA partners at the beginning of the consortium. Moreover, throughout the project, there were more than 100 people that contributed to the roadmapping process, either by directly editing the roadmap document or by providing input to roadmapping exercises initiated by the roadmap committee, whose results were incorporated into the roadmap. This large volume of contributions and contributors resulted in 13 scientific roadmap challenges and several other analyses achieved over 4 incremental roadmap releases. Such results could not have been achieved by the roadmap committee alone. However, having a central roadmapping committee was crucial to steer roadmapping exercises and to synthesize and integrate collected inputs from the broader community. We present in the following chapter several instruments that were used for roadmapping in SPARTA, and we outline their advantages and disadvantages while we applied them to develop the SPARTA roadmap.

[3] Deliverable D3.4: *Updated SPARTA SRIA (Roadmap v3)*, PU, M36
[4] SPARTA - D3.1 - INRIA_TUM-R-PU_M06-Finfal

1.4 Instruments for Roadmapping

The Roadmapping Committee relied on several instruments for steering discussions and collecting input from the SPARTA consortium on establishing and updating the roadmap. These varied throughout the lifetime of SPARTA, mostly due to the pandemic that started in 2020, which inflicted a considerable shift in the way teams collaborate and communicate. We describe in this chapter the lessons we learned during using these instruments for roadmapping in SPARTA.

1.4.1 Roadmap Challenge Proposal Form

In order to facilitate contributions to the SPARTA roadmap, we have designed a web form[5] and made it available to the cybersecurity community via the SPARTA website. The form was constructed as a questionnaire, with individual entries tailored to seamlessly build up into a cybersecurity challenge proposal that could be further integrated into the roadmap. This way, we intended to stimulate the SPARTA community and beyond, to submit their perspectives on cybersecurity with respect to achieving the mission of strengthening EU's digital sovereignty. The structure of the questionnaire resembled the individual points established in the template we used for describing roadmap challenges.

Essentially, we asked participants to map their proposed challenge onto the JRC taxonomy, as well as to break-down the challenge into more granular technological, education, and certification tasks, and finally to give an outlook on the impact of the challenge on digital sovereignty. We have then encouraged our cybersecurity community of partners and friends on several occasions to take part in the agile development of the SPARTA roadmap by filling out the questionnaire at both internal and external pilot events. This instrument did not stimulate participants to provide additional feedback to the SPARTA roadmap (we have received no submissions), potentially because the initially established roadmap has already identified the cybersecurity challenges that the EU should address to achieve digital sovereignty in a holistic manner.

1.4.2 Roadmap Challenge Ranking Form

The first version of the SPARTA roadmap was discussed thoroughly at internal events with the pilot partners as well as associates and third parties interested in the SPARTA mission. The result of these interactions was identifying a number of challenges that became central topics in the SPARTA roadmap. However, they were added in no particular order or priority. To assist policy makers within the EU in prioritizing investments in upcoming tender calls, we initiated a pilot-wide exercise to prioritize the roadmap challenges with respect to the mission of strengthening strategic autonomy in the EU. This prioritisation is based on input collected from the SPARTA network, and it had an online questionnaire[6] as main instrument that the roadmap committee used to conduct several surveying rounds.

Essentially, the questionnaire was designed with an entry for each roadmap challenge grouped in the three overarching categories exhibited by the SPARTA roadmap: Emerging Challenges, Transversal Challenges, and Program Challenges. Each entry encloses a rating scale ranging from 1 to 5: 1 representing a low priority, 5 representing a high priority, and 3 representing the (neutral) default value. Moreover, each questionnaire entry is followed by a text box intended to collect textual justification from the questionnaire users on their ranking. The latest roadmap version was made available to the participants for further assistance at all stages of the questionnaire.

We organized the first surveying campaign over the course of two months during which we received a total of 19 submissions: 15 from SPARTA partners and 4 from SPARTA associates & friends. However, this was merely a first step towards prioritizing the roadmap challenges. We note that the

[5] https://www.cybersecurityosservatorio.it/en/Services/sparta_roadmap.jsp
[6] https://www.cybersecurityosservatorio.it/en/Services/sparta_roadmap_grading.jsp

result might be biased because in this very first step, mostly SPARTA members were asked to prioritize. Nevertheless, the result shows an initial tendency for ranking. We have since carried several occasional surveying campaigns mostly within the SPARTA network, which produced 3 additional compilations: from 1 SPARTA partner and 2 from the SPARTA associates & friends. The cumulated results of these studies are summarized in Chapter 10 of the SPARTA roadmap[7].

1.4.3 SPARTA Workshops and Events

In close collaboration with SPARTA's Partnership Committee, the Roadmap Committee leveraged the various events organized for the SPARTA partners, associates and friends, to extend the roadmap based on feedback from the participating audience. Throughout the project, there have been more than 30 such events organized, accounting for a cumulated audience of around 2000 participants. Additionally, we took the opportunity to disseminate roadmap achievements during these events. Generally, the goals of these sessions were to:

- collect feedback on the existing roadmap challenges,
- rank existing roadmap challenges,
- brainstorm additional emerging challenges,
- disseminate roadmap results.

Several aspects spurred different types of SPARTA events. First of all, from the perspective of the target audience, SPARTA workshops can be classified in two types: national and pilot-wide. Second of all, 2020 marked the beginning of a major global pandemic, which impacted several classical habits, such as onsite meetings. As such, we have to classify SPARTA events based on the format of the meeting: onsite and online.

Although the roadmap and its questionnaires were presented relentlessly during the monthly national workshops, the response rate of the audience was generally lacking. We believe that this was mainly due to the peculiar nature of online meetings, as most national workshops have been organized remotely, even before the pandemic hit. This is perhaps unsurprising, as the reduced productivity of online meetings is, by now, universally known. Nevertheless, onsite SPARTA-wide workshops were significantly more productive because of the face-2-face interactions between the participants.

Under normal circumstances, we would have carried most roadmapping exercises in the context of onsite workshops. This was however not possible due to the shift to remote meetings. As such, in the second half of SPARTA, most calls for input and roadmapping exercises have been conducted online with SPARTA partners, associates and friends, mostly using the online questionnaires presented above. The results of remote exercises were, statistically, less effective, as we have received a significantly smaller number of compilations and reactions on the roadmap.

1.4.4 Feedback from Work Packages

Throughout the lifetime of SPARTA, several exercises have been carried with the scientific work packages of SPARTA for updating and extending the roadmap. For example, the roadmap committee was occasionally invited to the monthly meetings of the 4 scientific programs, where the rounds for contributions to the roadmap were introduced and discussed with the participating partners. Afterwards, each WP were given a few weeks to compile and consolidate the contribution to their respective roadmap chapter. All input was then collected by the roadmap committee and integrated into the roadmap. This form of interaction allowed us to have focused discussions on individual challenges from the roadmap, which the work programs were associated with. Moreover, it facilitated us to dive deeper into the program challenges of the roadmap and update them with detailed insights based on expert feedback. As such, the most substantial parts of the program

[7] Deliverable D3.4: *Updated SPARTA SRIA (Roadmap v3)*, PU, M36

chapters of the roadmap, including the granular tasks required to achieve it, are the product of focused interactions with work packages.

To stimulate the contribution of work package partners in a productive manner, we coordinated roadmapping exercises in three steps:

1. Introducing the exercise during a work package meeting including clarifications,
2. Collecting feedback from partners over the course of several weeks,
3. And finally synthesizing all the received submissions into the next release of the roadmap.

This form of exercise has been proven effective, as generally several submissions have been collected from SPARTA partners on the scientific roadmap challenge they were associated with.

In addition, it is worth mentioning that updating emerging challenges required a different workflow than scientific challenges. Specifically, the Roadmap Committee mostly nominated individual partners with expert knowledge to compile updates to emerging technologies, which were then synthesized, and circulated among the network for feedback.

1.4.5 Roadmap on the SPARTA Website

We have also published parts of the roadmap on the SPARTA website[8] in order to reach a broader audience. Specifically, we have extracted the 13 scientific challenges from the roadmap and projected them on an interactive timeline on the website where users can get an overview of their scope and steps. Additionally, we have published the questionnaires described in the previous sections on the same page as the roadmap, so that visitors can provide input asynchronously.

1.5 Inter-pilot Roadmapping

The 4 CCN Pilots and ECSO benefit from large individual networks of partners, including big companies, SMEs, universities, and cybersecurity research institutes, that join efforts into identifying cybersecurity research & innovation priorities for retaining EU's digital autonomy and sovereignty. Each consortium adheres to the common goal of strengthening and sustaining Europe's cybersecurity competence, but the 4 Pilots and ECSO take slightly different paths towards achieving it. After initial consultation rounds across the networks, it became clear that the different views on cybersecurity that individual agendas addresses are likely to complement each other in a fruitful way.

As such, shortly before the end of the first project year, SPARTA took the initiative to touch based with the other CCN pilots and synchronize on our individual roadmapping processes. The exercise started with a number of bilateral online calls where we exchanged experiences, achievements, and lessons learned until that time. During this activity, we learned the stance that the other pilots are taking on cybersecurity, and, interestingly, we have identified that our individual pilot perspectives have both common grounds and overlapping aspects. For example, other pilots have also developed cybersecurity roadmaps with focus on technological challenges for cybersecurity research and innovation, while some pilots addressed cybersecurity from additional angles, such as legal, economical, and societal, and others focused on cybersecurity challenges specific for selected sectors. Additionally, having the Commission's support, a structured focus group was assembled with members of all CCN Pilots and ECSO, with the aim to explore further inter-pilot synergies on consolidating a EU-wide cybersecurity agenda for strategic autonomy.

After several rounds of constructive discussions during the monthly meetings, the members of the roadmapping focus group have agreed on an initial, non-exhaustive shortlist of cybersecurity research priorities, critical for elevating the EU in cybersecurity in the upcoming decade. The consolidated list of challenges is the result of a careful analysis process that the focus group has

[8] https://sparta.eu/roadmap/

performed on the cybersecurity priorities of the individual agendas of the 4 Pilots and ECSO. The artefacts stemming from this activity have been forwarded to the Commission, and it was used to inspire the strategic recommendations made by ENISA to the ECCC[9]. Furthermore, the artefact was forwarded to the European Cybersecurity Atlas as well, which may assist the Atlas towards establishing a cybersecurity community within the EU that ought to grant it a leading position in the global cybersecurity marketplace. This was a first important step from a series of milestones that the roadmapping focus group aims to achieve towards integrating the different cybersecurity agendas being actively developed in the EU.

SPARTA played an important role in the results achieved so far in the roadmapping focus group, as it took coordinating role in initiating group discussions and exercises, as well as in centralizing and synthesizing inputs from the other stakeholders. Next, we are seeking further ways to efficiently produce useful recommendations based on our individual pilot results, and we may consolidate our views on specific cybersecurity challenges that individual sectors within the EU face. And lastly, we're discussing now the prospect of organizing a cross-pilot roadmapping event at the beginning of next year to disseminate the focus group's results achieved so far, and give an overlook into future outputs.

In summary, the open and agile roadmap development approach proved to be productive in SPARTA in terms of establishing and maintaining a comprehensive technological agenda for cybersecurity research and innovation. Although no major issues were experienced with this approach, we leveraged several tools for conducting roadmapping exercises that exhibited advantages and disadvantages. For example, face-2-face workshops benefited from a higher audience engagement than online interactions in terms of feedback on the roadmap. Nevertheless, asynchronous input via email or online surveys also produced quality roadmap contributions. Expectedly, a larger amount of input was received for the first iterations of individual roadmap challenges or chapters than subsequent iterations aimed to update them. Overall, we believe that SPARTA's initial objective of delivering a technological research and innovation agenda for strengthening digital sovereignty has been achieved. However, there are a number of additional challenges that need to be addressed in order to implement this agenda, as well as complementary aspects and angles that need to be considered besides technology in order to achieve digital sovereignty. We discuss all these in the following chapter.

[9] ENISA, *Proposals for the European Cybersecurity Competence Center*, 2021

Chapter 2 Future Assessment on Cybersecurity Roadmapping

In the previous chapter, we described SPARTA's roadmapping process where we outlined several lessons that we learned during the development of the SPARTA roadmap. We follow-up on those findings in this chapter, as we discuss the practices that we believe are worth keeping in future roadmapping exercises in the EU, as well as those that should be improved in order to maximize a roadmap's impact.

As already emphasized, there is no "one size fits all" in cybersecurity. As such, we recommend continuing to build roadmaps in a mission-oriented fashion with impactful missions for the EU. The mission of the SPARTA roadmap was to strengthen digital sovereignty. Due to the geopolitical situation we currently face, we strongly recommend sticking to that mission. SPARTA has taken a technology-driven approach by defining challenges that describe intermediate goals towards strengthening digital sovereignty, with sub-roadmaps defined for each challenge. However, the discussions in the Roadmapping Focus Group of the 4 Pilots has shown that it is valuable not only to take the technology-driven perspective, but also to develop roadmaps that have different angles in the focus, such as the user. In this way, various ways to achieve the global goal of digital sovereignty can be identified. This would open up further degrees of freedom that allow greater agility and the ability to flexibly adapt strategic decisions to changing requirements.

The open approach with bottom-up and top-down roadmap development was very productive throughout the roadmapping exercises carried by SPARTA. This facilitated a large volume of contributions and contributors, that resulted in several quality information integrated into the roadmap. The produced roadmaps could not have been feasible to a single roadmap committee, nor they could have benefited from coherent structure without it. Thus, we believe that this approach should be continued in further cybersecurity roadmapping exercises within the EU, especially in the upcoming cybersecurity landscape governed by the ECCC and the NCCCs. Such a cooperative model has already been tested in the roadmapping focus group, coordinated by SPARTA and made of members from the all CCN Pilots, ECSO, and the EC. On one hand, the EC provided hints on upcoming roadmapping activities at the ECCC/NCCCs that may benefit from the focus group's feedback. On the other hand, the members of the focus group conducted exercises and brainstorming sessions for collecting such feedback, which resulted in commonly agreed upon input forwarded to the ECCC/NCCCs. For example, encouraged by the EC, the roadmapping focus group identified a non-exhaustive list of research challenges that are of high priority for achieving digital sovereignty in the EU. This artefact was included by ENISA in the strategic recommendations report[10] that was forwarded to the ECCC. We believe that this collaboration model should be continued even after the pilots come to an end in order (1) to sustainably transfer the results of the pilots to the ECCC/NCCCs and (2) to benefit from input from the cybersecurity community in defining future agendas for cybersecurity. For example, overarching missions may be introduced by the ECCC/NCCCs in a top-down manner, while focus groups made of members from the cybersecurity community can provide feedback and recommendations in a bottom-up fashion.

Breaking down the overall mission into smaller, more granular milestones was definitely useful for implementing the agenda proposed by SPARTA, especially since cybersecurity challenges become so complex that they can very well merit a roadmap of their own. However, we suggest going even further in future roadmapping exercises and defining even more concrete and measurable goals on a mid- to long-term timeline (5/10/20 years). A hypothetical example would be: in 20 years 90% of all products should be secure by design and should be securely maintained by manufacturers over

[10] ENISA, *Proposals for the European Cybersecurity Competence Center*, 2021

their entire product lifetime. Additionally, the SPARTA roadmap prioritizes the scientific challenges that are required for achieving digital sovereignty in the EU, based on input from the SPARTA network. Specifically, topics like “Secure and Fair AI Systems”, “Trustworthy Software”, “User-Centric Data Governance”, “Full-Spectrum Situational Awareness” are of utmost priority for achieving digital sovereignty based on the collective perspective of SPARTA, and should, thus, be more in the focus in future EU projects. Nevertheless, we emphasize that the other scientific challenges proposed by the SPARTA roadmap are of high importance as well in order to benefit from digital sovereignty.

The SPARTA roadmap evolved over two major phases that differ quite significantly in terms of team collaboration environments: the pre-pandemic and during-pandemic periods. Before the COVID-19 virus emerged in early 2020, the foundation of the SPARTA roadmap along with its extended releases until that point were laid at SPARTA workshops organized on site. After the pandemic started, all input was collected via online forms, online conferences, or simply, via email. We observed that the former kept the audience more engaged and stimulated their creativity for a higher quality contribution to the roadmap. The later was empirically not as productive, however, it did produce useful results. This could perhaps be a side effect of the fact that the bulk of the roadmap document was already established in the early stages of SPARTA, thus, leaving little opportunity for improvements. As such, we strongly recommend organizing focused workshops with clear exercises for roadmap in an on-site fashion, while also occasionally collecting input from the community via online means.

The SPARTA roadmap mostly focused on identifying technological challenges required to achieve the mission of digital autonomy. Albeit technologies propel the evolution of our societies, cybersecurity is not solely a technological problem anymore. Rather, in order to benefit from robust and wide-spread cybersecurity several other aspects should be considered in roadmaps, such as legal, societal, and economical challenges. For example, we need to incorporate cybersecurity in the various existing business models so that it becomes a competitive advantage. Currently, adopting cybersecurity is perceived as slowing down manufacturing and delivery, which becomes a competitive advantage for those that omit it. Additionally, we need to have usable cybersecurity that ought to take unexperienced digital users out of the loop. Complex security is one of the weaknesses that for example phishing attacks abuse, while unusable security reduces the motivation to adopt it.

As emphasized earlier, cybersecurity is more than just a technological problem. Great amounts of research have been carried in cybersecurity over the years, yet, we still do not witness a wide-spread adoption as cyber-attacks continue to rise. For that, we believe that roadmaps focused on technology could benefit from guidelines for transferring research into practice. For example, much research turns into open source software and hardware. Open-source philosophies are generally perceived to align with EU’s trustworthy standards. However, the security of open-source products is not guaranteed unless there is a vibrant community built around them, constantly incentivized to maintain them, such as the Linux kernel’s.

Finally, we would like to point out that an iterative and agile roadmapping approach is highly advantageous. We therefore recommend that the ability to adapt flexibly should be taken up in the further development of the roadmap. The current geopolitical turning point due to the Ukraine war, as well as the Covid-19 pandemic, have illustrated the high technological dependency of the European countries on IT products from non-European providers. Against this background, the technology focus pursued in the SPARTA roadmap for research and development of key technologies to strengthen strategic autonomy has been confirmed. The prioritization of trustworthy, secure hardware, trustworthy data rooms, and trustworthy AI systems made in the roadmap is essential in order to give European companies and state institutes the ability to act independently. In the next iterations of the roadmap, we strongly recommend giving more priority to the question of developing resilient software and hardware architectures. The question of cyber defense has gained enormous importance in the course of current developments, so that measures to detect attacks, but also measures to develop system architectures in accordance with the principles of zero trust, are becoming significantly more important. We recommend that in the next iterations of the cybersecurity roadmap, more focus be placed on the technological challenges of resilience, risk mitigation measures and business continuity. However, the geopolitical development also shows that data and information have a decisive influence on opinion-forming and decision-making. The

topic of fake news and deep fakes has also increased in importance. We therefore recommend giving this topic more priority in the future cybersecurity roadmap.

As mentioned earlier, the Roadmap Committee of SPARTA exchanged ideas throughout the project with the other CCN pilots and ECSO. This has proven very useful and informative. We identified that SPARTA's technological focus could be very well complemented by other angles of cybersecurity that the other communities work on. Aspects include sectorial, social, legal, and economic challenges that cybersecurity poses. As such, we believe that the EU should continue incentivizing the cybersecurity community to work collectively for providing input on cybersecurity from different perspectives.

Chapter 3 Conclusion

In this document, we first presented the lessons that we learned while building and maintaining a strategic research and innovation roadmap throughout the SPARTA project. SPARTA adopted an open and agile roadmap development approach, with several roadmap development iterations that were based on input and feedback collected from the whole network of partners, associates, and friends. This turned out to be productive in SPARTA, as the final roadmap release elaborates 13 scientific cybersecurity challenges and several other analyses that aim to strengthen EU's digital sovereignty. Having the central overarching mission of strengthening digital sovereignty in SPARTA allowed defining and constructing roadmap challenges in a focused manner. Contributions to the roadmap were collected in a hybrid top-down and bottom-up manner in SPARTA. On one hand, a roadmap committee formed of principal roadmap stakeholders defined the overall SPARTA mission and the technological challenges of high priority to achieve it. On the other hand, the whole network provided detailed input for each roadmap challenge in a bottom-up fashion, which enhanced each challenge with concrete steps and milestones to achieve it.

Based on these findings, we then laid out several recommendations for improving future roadmapping exercises in the EU. Firstly, we believe that the cybersecurity community that formed the pilots should still be involved in the future roadmapping exercises of the ECCC/NCCCs, in a hybrid top-down and bottom-up manner. Secondly, we recommend continuing to define future roadmapping exercises in a mission-oriented way, as this approach allows identifying tailoring in cybersecurity challenges for achieving particular objectives, such as digital sovereignty. Thirdly, several cybersecurity challenges received a higher priority in the ranking proposed by SPARTA, and, should be given more attention in future projects. Finally, policies and economical models should be identified so that cybersecurity becomes a competitive advantage for the various industries, thereby increasing their willingness to adopt it.

We end up with the concrete recommendations to give more priority to the challenge of building resilient software and hardware architectures. We also recommend giving higher priority to the topic of combating targeted disinformation, including deep fakes, in the future Cybersecurity Roadmap,

Finally, based on our experience with building the SPARTA roadmap, we recommend setting up an expert group to accompany and supervise the process of developing a mission-driven cybersecurity roadmap in the EU. The group should take care that the various focal points, like sectorial, social, legal, and economic questions that are relevant for Europe are incorporated into the further development of the roadmap.

Chapter 4 List of Abbreviations

Abbreviation	Translation
CCN	Cybersecurity Competence Network
JRC	Joint Research Centre
WP	Work Package
ECCC	European Cybersecurity Competence Center
ECSO	European Cyber Security Organization
ENISA	European Union Agency for Cybersecurity