SPARTA

D1.5

Preparing a CCN pilot to become a sustainable CCN

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	41 months
Programme	H2020-SU-ICT-2018-2020

Deliverable type	Report
Deliverable reference number	SU-ICT-03-830892 / D1.5 / V1.0
Work package contributing to the deliverable	WP1
Due date	May 2022 – M40
Actual submission date	22nd September, 2022

Responsible organisation	CEA
Editor	Florent Kirchner
Dissemination level	PU
Revision	V1.0

Abstract	This deliverable reports on how governance, R&D&I, community and exploitation activities have been prepared for sustainability.
Keywords	Policy capacities, Research governance, Mission-oriented innovation, Leadership management, Collaboration incentives

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

Editor

Florent Kirchner (CEA)

Contributors (ordered according to beneficiary numbers)

Thibaud Antignac, Augustin Lemesle, François Terrier (CEA)

Philippe Massonet (CETIC)

Jan Hajny (BUT)

Dirk Kuhlmann, Michael Friedewald (FHG)

Herve Debar (IMT)

Fabio Martinelli (CNR)

Evaldas Bruze (L3CE)

Bertrand Lathoud (SMILE)

Marek Pawlicki, Damian Puchalski, Michal Choras (ITTI)

Goncalo Cadete, Elisabete Carreira, Catarina Valente (INOV)

Reviewers (ordered according to beneficiary numbers)

Lukas Malina (BUT)

Volkmar Lotz (SAP)

Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author`s view – the European Commission is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

Executive Summary

This document presents the various ways in which SPARTA has prepared its governance mechanisms, large and small, to become sustainable through transfer to a Cybersecurity Competence Network.

By building on the continuous feedback performed during the lifetime of the project, and on the experiments led by Program and Activity leaders throughout year 3 and beyond, SPARTA provides a set of concrete instruments for the sustainable operation of network operations.

Table of Content

List of Figures

List of Tables

Chapter 1 Introduction

1.1 Purpose

This document aggregates and synthesizes contributions from SPARTA programs, activities, and governance leaders. It reports on how governance, R&D&I, community and exploitation activities have been prepared for sustainability throughout SPARTA's final months of operation. It is meant to convey key lessons and ongoing follow-up actions to the Commission, the ECCC, the NCCs, and any reader interested in applied, innovative governance policies.

1.2 Context Update

Proposal COM 2018/0328 "for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres" has entered into force in June 2021.

This has triggered the launch of the ECCC, with a number of decisions setting the stage. First, the decision by the Council to establish the Centre in Bucarest, continuing a trend in decentralization, and acknowledging – almost presciently – the stake of an eastern implantation of cybersecurity assets. Second, the administrative setup of the ECCC, under the interim stewardship of Unit H1 at the European Commission. This started in particular with the setup of the Governing Board, including a modus operandi and the adoption of a strategic document for 2021 and 2022. This also covered a variety of practical questions, for instance with regards to the elaboration of EU funded activities, for which ENISA prepared a recommendation "The Way Forward Report", synthesizing inputs from the 4 pilot projects, ECSO, and the joint focus groups. This will help in preparation for the 2023-2024 work programme, which will be the opportunity to align existing draft WP with the Centre on the one hand, and with Member States priorities on the other hand.

At the beginning of 2022, following the designation of NCCs by their respective Member States, work quickly started with questions on the constitution of the Cybersecurity Community: how to manage the community, how to register its members, which requirements to impose on membership, etc. While different views arose from the Member States, the Commission and Governing Board cultivated the idea of Member States leading the discussion, and developing specific guidance on membership choice and attractivity. NCCs have also started constituting their services catalog, and setting up organizational measures to handle their concrete implementation.

1.3 Structure of the document

The remainder of this document is structured as follows. Chapter 2 gives an overview of governance reactions to external and internal recommendations, and their impact. Chapter 3 reports on governance aspects for Programs and Activities, with a focus on synthesis and outlooks. Chapter 4 identifies skills and instruments required to sustain the modular governance of a high risk – high reward cybersecurity competence network. The final chapter 5 presents the conclusions.

Chapter 2 External recommendations

In this section of the document, we take the opportunity to discuss the recommendations received during the external assessment realised by Technopolis of SPARTA. These recommendations on SPARTA's governance were summarized and compiled here as well as the actions taken w.r.t. them, keeping in mind the requirements of a future European Cyber Competence Centre and Network and its sustainability. The recommendations themselves suggestions can be found integrally in deliverable D1.4 "Lessons learned from externally assessing a CCN pilot".

Table 1: Recommendations from D1.4

No.	Recommendation	Action taken, current status
1	Clarify the role of key governance bodies: • Roles of EB vs SD • Improve communication to all partners on the decision taken at these boards	The roles of the EB and the SD was clarified to the relevant members that might have still held some doubts whereas as the coordinator efforts were made to clearly separate strategic issues for the SD and executive issues for the EB that might have tended to get mixed in some points. Impactful decisions were communicated to the relevant partners, however it is worth noting that SD meeting decisions were mainly of direct impacts to its participants which then guided their action through them. On the other hand, EB decision remained purely executives and all necessary partners were informed of these decision to act upon.
2	Enhance internal communication • Improve communication between transversal and technical WPs.	See recommendation 1 for the WP12 actions related to this topic as well as recommendation 17.
3	Enhance outreach and external communication • Strengthen collaboration with other 4 pilot programs to share experiences. • Inform more clearly, how they can contribute, when and where they can see the impact of their contribution. • SPARTA should experiment with more thematic events fostering cross-border participation.	SPARTA kept up networking activities even in presence of pandemic, and fostered the cooperation with other pilots, both in terms of events and project activities. For instance, as the NeCS winter school that brings together all the PhD students and have a steering committee of all the 4 pilots. During these meetings hands on sessions in particular on the cyber ranges and other tools developed by the pilots are performed. Similarly the FOSAD PhD school is organized between several pilots. Overall the collaboration with the 4 pilot was followed with the different focus group of which some were initiated and led by SPARTA. As well as through various even organised together. SPARTA also strived, by inviting Associates and Friends to all relevant meetings through the mailing list and relaying information with monthly newsletter to them to include the whole community and to clearly show them how they could participate and their potential impact. A good example

No.	Recommendation	Action taken, current status
		here is the inclusion of SPARTA Associate and Friends into the Brokerage events.
4	Ensure learning from SPARTA experiences • Working on a common 4P policy brief on all relevant issues to be addressed in the context of ECCCN, including controversial ones. • SPARTA should consider a limited continuation to ensure dissemination, exploitation and transfer of SPARTA experience to ECCCN. This could take the form of a Horizon Result Booster project.	• Through the work realised by the EC supported by ENISA, SPARTA worked together with the other pilots and ECSO on providing inputs for a report on the way forward for the ECCC and the areas of focus. Meetings with the EC and the other pilot also remain opportunities to provide such inputs. SPARTA plans to continue participating to these meetings. • SPARTA was allowed for a 5 month extension to continue with action on dissemination, exploitation and transfer of experience to the ECCC (as other pilot also were finishing later). This for example took the form of new dissemination material and impact video being produced or a second exploitation hackathon being realised. Even after this 5 month extension, SPARTA plans to keep up some limited action such as experience transfer. Finally, some of the activities of SPARTA will continue outside of the scope of the project such as the training and education activities that will partially continue as part as the REWIRE project.
5	Strengthen SPARTA as a proper governance pilot • SPARTA should consider deliberate measures to gain further experience as a proper governance pilot.	This option was not explored as it proved too hard to explore in the current context and setting.
6	The challenge/feedback collection form is not optimal for data collection.	In addition to the challenge/feedback collection form based process, cross-alignment and roadmap update workshops have been introduced involving all programmes representatives as well other WP leaders and core team members.

Chapter 3 3rd year governance activities

During the third year of the project, SPARTA continued the work around the organisation of a Cybersecurity Competence Network (CCN). Still based around a modular governance as described in last year D1.3 deliverable, this section describes the evolutions that occurred around this framework. The evaluation and effectiveness of this governance and evolutions is discuss in three parts: on the CCN Structure itself in Section 3.1, for its transversal activities in Section 3.2 and for the scientific and technical activities in Section 3.3.

3.1 CCN structure

In this section, the new activities pertaining to the CCN structure itself that were conducted in the third year of SPARTA are described succinctly. In a first section the CCN structure of SPARTA is evaluated and discussed through a survey while the second section summarize the contributions of SPARTA's CCN structure and activities to the ECCC. A follow up of this section can be found in Chapter 4 where the CCN structure is thought around the aspect of sustainability and job description.

3.1.1 Satisfaction questionnaire

As part of the governance process of SPARTA, WP1 and CEA were tasked to evaluate the level of satisfaction of the network members with SPARTA's governance during the project. This task was initially envisioned through an annual survey based on the Likert Scale where the goal was set to 5 out of 7. This survey would serve as a good indicator of the climate inside SPARTA and of the efficiency of its structure. It would also allow some less implicated partners to easily relay any issue or suggestion to the SPARTA Governance and in turn, for the governance, to reach out and adapt to them.

A first survey was to be carried out after M12, January 2020, in order to evaluate the satisfaction over the whole first year. At that point, discussions were started on the methodology to be followed, and on the format and the content of the satisfaction questionnaire to be sent. Unfortunately, soon after, the COVID-19 pandemic put this process on hold. Following this, in the beginning of the second half of the Y2, the external assessment process was started and it was decided to mutualise the first and second year survey by relying on the external assessment made by Technopolis. The questionnaire was designed by Technopolis with the help of CEA in the scope of the procurement for the assessment and is presented in Chapter 8. This mutualisation was performed in order to reduce the overhead and the duplication of the solicitations to the SPARTA partners, associates and friends. In that sense, only one questionnaire was sent to the partners instead of three for Y1, Y2 and for the external assessment in the span of a few months.

The full methodology and results of the questionnaire sent by the Technopolis Group for Y2 are described in Part 2 of D1.4 "Lessons learned from externally assessing a CCN pilot" where the external assessment is described. The questionnaire received replies from 34 SPARTA Partners and 12 SPARTA Associates or Friends. The conclusions and reflexions on the results of this questionnaire are described in D1.4 and were taken into account for Y3 of the project. In order to map these results with the original KPI 1.3 on the satisfaction of SPARTA partners, we mapped the five levels of response to numerical values from 1 to 5 before rescaling the results to the Likert scale of 7. Thus, the results show an overall satisfaction level of **4.97/7** for the Y1 and Y2 of SPARTA.

For the third year of SPARTA, we decided to employ the same methodology and questionnaire as the ones from the Technopolis Group in order to obtain comparable results. The questionnaire was created and disseminated using the online platform CryptPad[1] and its form application. This iteration of the satisfaction survey received 42 answers, from 29 SPARTA Partners and 13 SPARTA Associates or Friends. With only 4 less participants, the results are comparable to the previous study.

[1] https://cryptpad.fr/

Additionally, in the respondents, 10 work package leaders were represented. Overall, the level of satisfaction measured reached **5.14/7** which shows an improvement compared to Y1 and Y2.

We can draw some tendencies from looking at the results of the questionnaire. First of all, the comments left at the end of the questionnaire mainly reflect the need for more internal communication among the consortium and internal dissemination of information and results while highlighting that physical meetings might have brought more coherence to the project and to its results which suffered from the COVID-19 pandemic. This is also shown with the results on communication among partners (Question 7.vii), which scores the lowest in the questionnaire with 4.11/7. While efforts were made from WP12 and WP13 on strengthening internal communication through internal newsletters for example, and from WP8 on communicating with SPARTA Associates and Friends, we believe that the needed effort for internal communication was underestimated at the time of the proposal and more concrete means of information were to be created for the quantity of information generated in SPARTA to be properly disseminated to all partners. More systematic channels of news for the results and effort to populate them need to be planned in a consortium of this scale and they need not to strain communication. Additionally, this should be paired with the necessary channel for information gathering which might be seen as a burden in such a large consortium. This has been one of the topic of discussion in WP13 to disseminate information but also in WP10 to improve the gathering tools and strategies such as mutualising all requests for information were also tested in SPARTA as a whole.

For SPARTA Partners, the highest score are for the number of opportunities to provide inputs to SPARTA's technical and non-technical activities (5.86/7), showing the good dynamics inside all of the SPARTA WPs, and the importance of a WP focused on ELSA (5.85/7). The latter has increased since Y2 underlining the efforts made by WP2 on mainstreaming ELSA practices.

On the SPARTA Associates and Friends side, the results show that they rate the inclusiveness and openness of SPARTA highly (5.91/7 and 5.77/7) while still estimating that the network would benefit from more opportunities for them to discuss and provide inputs to the different activities (4.57/7). Unfortunately, on that question, opportunities were limited by the pandemic which restricted the physical interactions more adequate for discussion but also by the available efforts and the context of an H2020 project that limited the interaction with new partners without doing heavy manoeuvres to add on the Description of Action. Nevertheless, some interaction with external associates were held in the scope of the T-SHARK Program.

The answers "Don't know" were excluded from the previous numbers but we can note that on average for SPARTA Partners, Associates and Friends, the proportion of people answering "Don't know" was of 11%.The questions with the largest proportion of people answering this were the 2 questions related to the Strategic Direction (SD) for the SPARTA Partners, showing still a slight disconnection between the discussion held in the SD and the whole consortium. For the SPARTA Associates and Friends no particular question was above the others on this point.

In summary, this form of survey proved to be a good way to gather feedback and improve from the comments of the partners in SPARTA. It provides an efficient medium to gather information on the overall satisfaction in the project and its governance but also brings a good level of granularity to identify, either through comments or low scores, key issues that might needs actions. Nevertheless, while this questionnaire needs only a few minutes to fill some effort still need to be spent to gather inputs with periodic reminders. Ways to motivate the participants to answer might be found in showing them the follow-up actions of the questionnaire.

3.1.2 Mapping to the European cybersecurity strategy

As part of the initial proposal of the project, SPARTA proposed to follow the contributions of the different activities to the general objectives of the project through KPIs, as well as to map these contributions and objectives to the European cybersecurity strategy. This mapping would serve to link the CCN pilot to the overall European cybersecurity strategy in a sustainable fashion.

At the same time, the European Commission with the support of the ENISA, aimed to define a strategic agenda as well as a multi-annual work programme for the European Cybersecurity

Industrial, Technology and Research Competence Centre and Network of which SPARTA is a pilot. Through a collection and combination of inputs amongst SPARTA, the other 3 pilots and ECSO, the way forward and priority areas were defined by the EC and ENISA to improve cybersecurity in EU. These conclusions are compiled in a comprehensive and private report including SPARTA contributions and mapping of activities. As such, SPARTA contributed with its different activities, past, present and future, to this strategic agenda of the European cybersecurity, effectively mapping the CCN pilot's objectives and inscribing them in it. In turn, this will guide SPARTA's alignment with this European strategy and the sustainability of the CCN.

Overall, this exercise has proven to be a good support to align the strategy of the CCN and of its various activities. It might be beneficial to consider periodically reassessing all ongoing and planned activities in the CCN in such fashion to better align the activities and the overall strategies. This exercise was also the opportunity to show through the input gathering how their activities are registered in the current strategy and make them adhere to this strategy, answering potential disconnection found for example between the SPARTA SD and all the partners. While this exercise is good it should not be a strain on the activities themselves and should be well planned and understood from all parties and done through pertinent means and tools. In the limited context of a CCN pilot like SPARTA by itself such a complete report as the one produce might be out of scope as it demands a lot more efforts than what was planned.

3.2 Transversal activities

This section of the report is dedicated to SPARTA's transversal activities. SPARTA's transversal activities include the community and exploitation activities, i.e. WP8-WP12 as well as WP2 ELSA activities:

- WP2 – Responsibility activities
- WP8 – Partnership instrument
- WP9 – Cybersecurity training and awareness
- WP10 – Sustainable exploitation and IPR
- WP11 – Certification organization and support
- WP12 – Dissemination and communication

In this section, we report on the key governance and management takeaways during the third year of SPARTA keeping in mind the initiatives and recommendations that were reported in deliverable *D1.3 – Improving a CCN pilot* and *D1.4 – Lessons learned from externally assessing a CCN pilot*, as well as to other initiatives that contributed to improving the activities and processes in scope, including inter-pilot activities.

The focus in Year 3 turned towards the future CCN (ECCC/NCCC) setup and operation as well as its sustainability.

In the following sub-sections, a report is provided for each of the ELSA, community and exploitation activities. After reminding the context and previous observations through a gathering of previous deliverables, the pilot governance and execution considerations from Year 3 are reported.

3.2.1 Responsibility activities

The governance of the Responsibility Activities (WP 2: Responsible innovation: ethical, legal and societal aspects) was based on three main pillars: 1) a dedicated activity following its own work programme, 2) social and legal scientists embedded in the technical activities and 3) (limited) involvement of all other WP leads. This basic concept has proved to be robust.

The dedicated scientific work of the responsibility team was intended to make sure that social, ethical and legal issues are identified early and addressed in a comprehensive manner. One of the lessons learned from SPARTA was that most of the technical programs – especially those doing more fundamental research - have not (yet) developed a sense of the potential applications and their implications. Therefore, it is important to have Social Science & Humanities (SSH) and legal experts

that analyse developments from the political and societal spheres with a view to their significance for cybersecurity and to communicate them to the technical community in an actionable form.

In addition, a dedicated work package gives ELSA due visibility within the governance of the overall project. Thus, the treatment of ELSA is not automatically perceived as a mere service; this results in a stronger identification of the involved partners with the mission of the whole project.

In order to actually influence actual design decisions, the concept of the *embedded social scientists* (sometimes referred to in the literature as "embedded humanist" or "engagement agents" [1, 2]) who are continuously involved in the development process and thus much closer to the decision-making locus. They are no longer just distanced critical observers, but become more influential insider agents who identify problematic aspects of the developed technology at an early stage and work out possible solutions together with the developers.

In order to perform this function effectively, however, an appropriate process is necessary to ensure that relevant information is provided in a timely manner and that interaction between technology developers and ELSA researchers takes place at (least at) well-defined times. As other elements of the WP 2 work program could not be implemented as planned due to the Covid-19 pandemic, this was the most productive part of the SPARTA responsibility activities, leading to numerous practically useful results for the technical program (as documented in Deliverables 4.5, 6.1, 7.1, 7. And 7.3).

In order for responsibility activities to be successfully implemented, a number of requirements must be met. The first requirement is the right degree of specificity: It was naive to believe that there is a small number of guiding rules that are universally valid and implementable at the same time – a critique recently also formulated about the numerous "ethics guidelines" for AI [3]. It is therefore important to provide for the elaboration of concrete application-specific questions in addition to general advice, as is often given by typical ethics advisory boards.

The second and decisive factor for success is commitment and participation. Therefore, ELSA must be considered an integral part of the overall development plan from the very beginning, taken as seriously as functional requirements in the implementation. To this end, there must be a commitment from the leading person who makes sure that all stakeholders are providing the necessary input.

Results in a nutshell

- **Governance of ELSA**: ELSA must be considered an **integral part** of the overall development plan from the outset and taken as seriously as functional requirements during implementation. A separate work package gives ELSA appropriate visibility within the governance of the overall project. Thus, the processing of ELSA is not perceived as a mere service - this leads to a stronger identification with the mission of the overall project.
- **Design of ELSA**: An appropriate process must be defined to ensure that relevant information is provided in a timely manner and that interaction between Embedded Social Scientist are no longer just detached critical observers, but become **influential insider agents** who identify problematic aspects of the developed technology at an early stage and work with the developers to identify possible solutions.
- **Experts of ELSA**: It is fundamental to have SSH and legal experts who can analyze developments from the **political and social spheres** in terms of their relevance to specific topics.
- **Putting ELSA into action**: It is therefore important to provide for the development of concrete **application-specific issues** in addition to general advice, as is often given by typical ethics advisory boards.

3.2.2 Partnership instrument

After the launched of the SPARTA Associates & Friends program in the first year and the effort to consolidate the SPARTA activities in the different national cluster during the second year, the third year activities consolidated the SPARTA Associates & Friends program through a series of events

and joint proposals and initiatives. During this period, several countries set up their national coordination centres for which SPARTA with its partnership programme contributes to consolidate their network and ease communication among national and European partners. Through the Partnership Committee, these actions are organised, promoted and synchronised with all partners and national representative as well as with the strategic consideration of the Strategic Direction.

Strong of its 44 partners and near one hundred Associates and Friends, the SPARTA community held several plenary meetings, either in the form of SPARTA Days or of SPARTA Brokerage events. At the last brokerage event in June 2021, more than 110 participants registered and presented their activities. Similarly, SPARTA monthly meeting were performed in European countries with SPARTA partners or on request of other communities, for instance in Switzerland.

However, only a minority of these events were organised in a physical fashion, during the first year or with a timid come back during the end of the third year. Thus, although in terms of number of events and participant those events are interesting, only physical presence can guarantee the proper level of feedback and interaction inside the community. Nevertheless, these events supported the creation of a wider innovation community linked by the SPARTA network with national communities able to cooperate at European level.

To support this community, the SPARTA Joint Competence Centre Infrastructure (JCCI) was continued in the third year with the main goal of having more members deploying their nodes and taking part in this infrastructure. The distributed architecture developed in the first and second year indeed allows for members of the community to run locally their services as a JCCI node and share them to all JCCI partners. A final implementation allowed the extension of the JCCI to include hands-on-labs and share interactive service directly inside the JCCI.

With respect to its integrated services, the JCCI already embodies some of the tools developed in the programs or in transversal activities such as training framework and includes cyber ranges solutions. Some services are provided by Associates or Friends through the JCCI and several tools are already used by partners and Associates/Friends. Overall, this shows that the JCCI can serve as an efficient basis of support for the community to share its results and capabilities.

Finally, in terms of cooperative activities, the services of the JCCI and the enlarged community for Associates/Friends are useful both to produce new project proposals through the aforementioned Brokerage Events but also with letters of support from SPARTA to selected projects. This early support and liaison with budding proposal allows to foster networking activities from an early stage and strengthen the links inside the community through these projects. Nevertheless, we observed that while some cooperation resulted in strong collaborations (with REWIRE, SAPPAN … as reported in D8.3), the follow up after the letter of support would need to be more prominent to concretize all these cooperations. On another note, cooperation with ECSO and the three other Pilots, driven by the Commission has been successful; in particular the last CONVERGENCE and CONVERGENCE Next events represents a success story of cooperation. Similarly, the NeCS winter school that was planned immediately in Jan 2020 and 2022 despite the pandemic, with the contribution of all the 4 pilots was one of the first event to consolidate young researchers cooperation as well as joint event organizations.

Figure 1 and Figure 2 below shows how with the SPARTA partnership program SPARTA was able to increase the representation of the European community. The first picture is just with SPARTA partners while the second also with associates/friends.

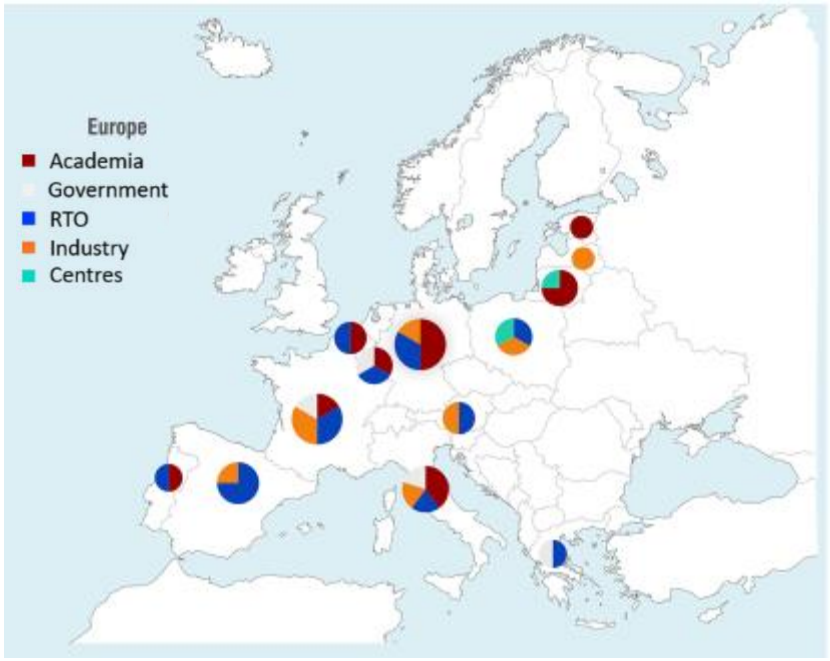

Figure 1: SPARTA Partners repartition in Europe

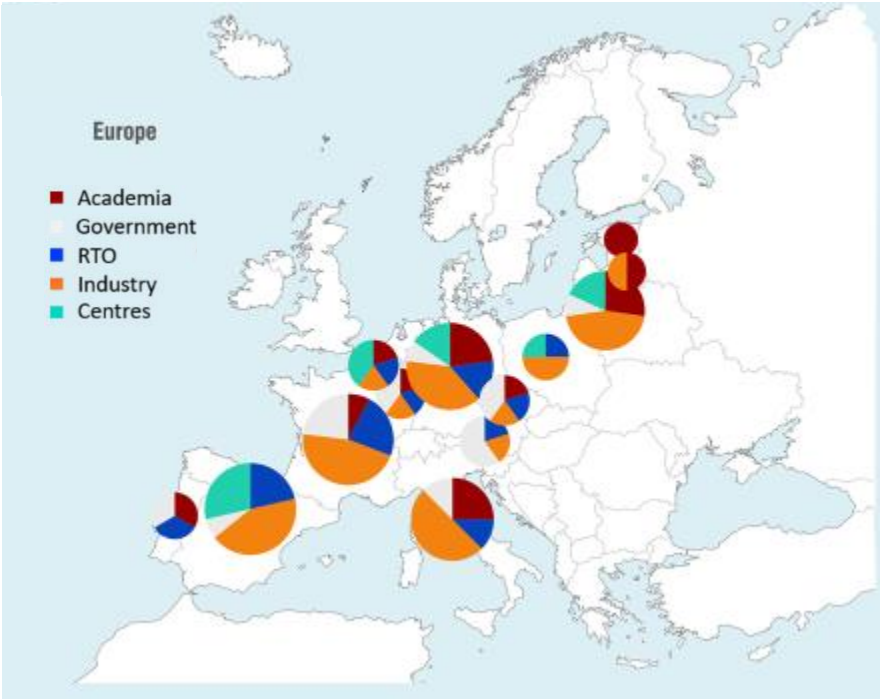

Figure 2: SPARTA Associates and Friends repartition in Europe

3.2.3 Cybersecurity training and awareness

In 2021, the WP9 activities moved from the design and development phase to the implementation phase. Most of the activities were focused on the piloting of cybersecurity courses and trainings, the production and deployment of tools for the support of education providers and the collaboration with

key partners, ENISA in particular. SPARTA WP9 also significantly focused on the sustainability of its results, not only creating the tools, but also finding the partners for their maintenance after SPARTA project is finished. In this aspect, ENISA turned out to be the most important partner for both course mapping activities and skills framework activities.

Regarding the collaboration with other SPARTA work packages, the most intensive work was with WP8 on JCCI and WP12 on Go Cyber with SPARTA.

Together with WP8 members, we worked on the integration of BUT's cyber-range installation with the JCCI portal, allowing the external access to BUT training resources. This activity involved the coordination and collaboration with other pilots too, mostly with CONCORDIA. Together with CONCORDIA partner Masaryk university, we deployed and evaluated the open source KYPO tool (which later this year won the European Commission's Innovation Radar prize). Throughout the year 2021, we worked closely with the CONCORDIA team on the testing and benchmarking of new features of KYPO.

Together with WP12 members, we organized workshops within the Go Cyber with SPARTA initiative, we were able to deliver cybersecurity training workshops at European outermost countries. WP9 was responsible for the coordination, creation of training materials and delivering the workshops to trainees from the critical infrastructure industry, digital innovation companies and education providers. Go Cyber with SPARTA is one of the activities that gained a lot of positive feedback from trainees and is considered for extension.

On the collaboration and governance involving external partners, WP9 was mostly active in the Education Inter-Pilot CCN Group, where it focused on the development of the Cybersecurity Skills Framework and the organization of networking and governance activities. One of the most welcome events was the ETACS workshop organized by SPARTA WP9 where all CCN pilots, ENISA and NIST participated and discussed the further development of Cybersecurity Training and Education.

The collaboration with ENISA was further extended as two WP9 members became members of the ENISA EU Cybersecurity Skills Framework, where the experience and past knowledge from the SPARTA CSF was used. SPARTA WP9 is still highly active in this group and significantly influence the creation of the novel EU Cybersecurity Skills Framework. The next steps concerning EU CSF and focused on practical impact were already planned for SPARTA extension dealing with the newly deployed tool SPARTA Curricula Designer.

3.2.4 Sustainable exploitation and IPR

Following up on the initial idea, the platform, called RAMP (Research Assets Management Platform) was brought online in December 2020. It allowed to experiment with the various forms that had been implemented (APER – Assessment of Pre-Existing Resources), DMP (Data Management Plan), and IDPR (Identification and Documentation of Produced Results). Three more forms were created: one for Privacy analysis, another related to Intellectual Property management, and the latter focused on Security requirements. The idea was to simplify the work of researchers when creating reports, such as the DMP, as they would be the collection of each individual DMP per asset used in the research. And once done, it could be re-used in several research projects, as needed.

Given its purpose, i.e. to make the wider community benefit from it, it was decided that it would fit under WP8, as a direct contribution from SMILE to both JCCI and Community fostering.

Practically, if the RAMP V1 allowed to quickly acknowledge that the foreseen features were both feasible and usable, it also highlighted serious issues on the architecture of the platform itself. As the proof of concept had been built on top of MISP, it inherited its properties. And this became a source of concern as the purpose, even if sharing widely, was not constrained in the same way. The main problem revolved around the granularity of authorization and authentication functions related to individual roles.

After some iterations, the developers concluded that it would not be possible to go further in adapting MISP and it was decided, in the second half of January 2021 to proceed with a completely new architecture. This led to the design and implementation of the RAMP v2. It was brought online in August 2021, and made available to the JCCI in September, for a wider adoption.

WP10 supported actively the request of the Project Officer during the formal review of February 2020 to have SPARTA focusing more closely on maximising its impact on strategic autonomy, by generating a structured approach to do so in a practical manner. It was shared with the Strategic Direction Board in November 2020 and used as a starting point to develop a questionnaire for researchers that was later added to RAMP.

Another issue arose in 2021, with the lack of progress on the KPI's for WP10. That is mostly one of the consequences of the COVID19 Pandemics, which did not allow more "in-person" interactions, which would have been particularly needed to brainstorm on what would be the most realistic paths to create start-ups from the results of the different research activities.

It was addressed through several paths:

- A more aggressive communication during Executive Board meetings allowed to get higher attention to the issue from most of the Work Packages
- In cooperation with WP8, a workshop was ran online on the 22nd of June 2021, focusing on Strategic Autonomy and Exploitation.
- Another workshop was conducted online on the 9th of November 2021
- And finally, two Hackathons aimed at generating start-up ideas was organized in January and May 2022.

All these actions allowed to complete and go beyond the target of the KPI 7.2. Progress was made on KPI 7.1.

Finally, the work on Deliverable D10.5 and D10.6 allowed to refine the approach of exploitation, with significant work conducted on how to maximize impact of exploitation on EU Strategic Autonomy, as requested by the Project Officer during the Formal Review of February 2020. Under D10.5. an Exploitation Roadmap was developed that uses the TRL scale as a basis for strategic and standardized decision-making when planning exploitation activities and technology transfer activities of research outcomes.

3.2.5 Certification organization and support

As planned in year 3, the certification organization and support activities have continued cross-cutting collaboration with the CAPE and HAII-T research programs. Preliminary contacts with T-SHARK and SAFAIR have been established but showed that collaboration on certification was not a priority for these programs.

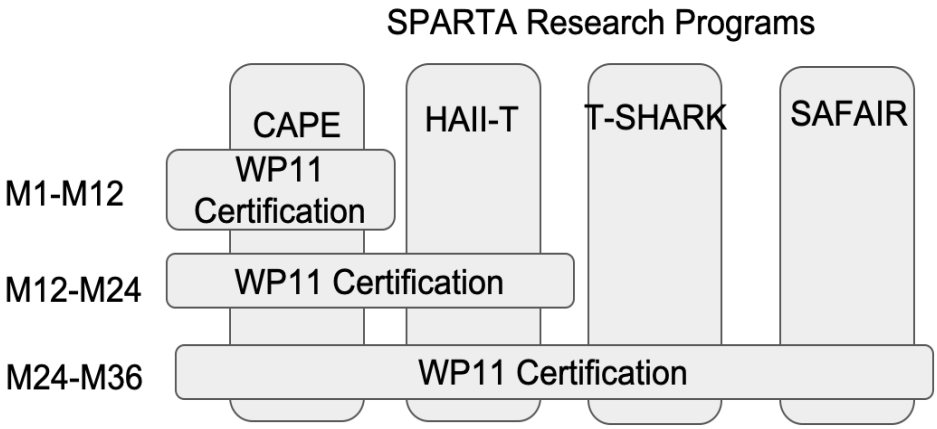

Figure 3: Status of cross-cutting certification activities

Figure 3 shows the cross-cutting certification activities with the research programs over the periods M1-M12, M12-24 and M24-M36. The activities with CAPE have started at M1 with the topic of efficient certification processes and incremental certification and led CAPE certification effort towards these goals by integrating incremental certification processes into cybersecurity assessment processes. Collaboration between WP11 and CAPE continued in the context of T5.4 covering both product as well as process certification, which was the focus of D11.2.

At the same time and after a state of play w.r.t. HAII-T and certification during M12-M24, cross-cutting certification activities with HAII-T have continued with T6.5 on the topic of GDPR compliance. T6.5 is developing a requirements tool to verify compliance of a process with respect to GDPR. This tool is only focused on the requirements stage. The content of the discussions are related to how their GDPR tool could be integrated into a DevSecOps process and become part of a certification tool chain. While some difficulty was found in the fact that WP11 partners were not involved in the HAAI-T program like in the CAPE program, the discussion between the two have triggered a lot of interest and will be considered as future work. As pointed in D11.5, the area of IoT as been marked as a priority for preparing cybersecurity standards, thus the work realised here is inscribe in a much wider cybersecurity strategy.

Interaction with national cybersecurity authorities involved in SPARTA on the topic of certification is the topic of T11.2. Individual meetings were planned and occurred with the national cybersecurity authorities in the M24-M36 period. Topics of interest have focused on preparations of the NCCC and the lessons learned from SPARTA.

The discussion on the conformity assessment bodies planned in the EU Cybert Act have been the topic of discussion with the national authorities involved in SPARTA. Nevertheless, it has remained very preliminary as the first cyber act draft certification schemes are still in the preparation phase and have not been rolled out. Further discussion on this topic have been produced in deliverable D11.3.

3.2.6 Dissemination and communication

From the strategic axis defined in the beginning of the project, the communication and dissemination activities, during the third year, ensured the continuity of the both the “Awareness” and “Participation” axes. While both these axes remained impacted by the COVID-19 pandemic, workarounds with virtual or hybrid participation allow to avoid any major roadblock to the implementation of these axes.

The pandemic has also been an opportunity to rethink the solution proposed in building and organising these axes with new solution and interaction possible. The activities also contributed to impact on attitudinal behaviour, that is of public interest, towards cybersecurity actions such as the 1) adoption of cybersecurity habits 2) the acquisition from the industries of cybersecurity services; and 3) academy starts to direct their interests and activities towards the issue. This was possible mainly through task 12.4 *Closing the Gender and Diversity Gap* and task 12.5 *Outermost Regions Engagement – “Go Cyber with SPARTA” campaign that* promoted several positive actions for cybersecurity awareness building. These activities and their impact are detailed in D12.6 and D12.7.

During the three years of the SPARTA project, SPARTA members participated in 70 conferences/workshops/others, organized 17 conferences and 40 Monthly Workshops, through both virtual platforms and on-site events. Most of these events occurred at the international level and gathered a significant diversity of stakeholders, from industry to research and academy. SPARTA partners have additionally published 126 scientific papers.

The C&D strategy adopted for the SPARTA social media accounts and the updates established in deliverables D12.3 and D12.4 has contributed to the project’s visibility and to the engagement of target groups with the SPARTA values, goals, activities and results. It helped to achieve 1290 followers on Twitter, 586 on LinkedIn, and 240 on Instagram, and create a SPARTA community.

The SPARTA website has been often updated and worked on during the whole project lifetime, in a collaborative work between all WPs, led by INOV and CEA, to ensure SPARTA delivers a dynamic,

intuitive, and complete platform to its visitors. Different sections of the website present the results, events, news and any other information on the SPARTA project such as the JCCI, the Gender and Diversity campaign or the Training and Awareness.

The SPARTA gender and diversity dimension has been enhanced during this period, allowing for more incisive actions and collaborations, namely with the Women in SPARTA campaign, related posts on social media, the event "SPARTA: The Future Needs You!" and the deployment of the Best practices guide for attract and retain women in Cybersecurity teams.

WP12 strived to build even straighter communication flows within the SPARTA Network to ensure that the SPARTA impact is duly communicated to the SPARTA stakeholders. These straighter communication flows aimed at responding to the reported difficulties by WPs related to internal communication as being a roadblock on some tasks. WP12 created the SPARTA News, a monthly internal newsletter to ensure partners, associates and friends are aware of all the activities and results developed in SPARTA, and that all WPs contribute to its creation.

Overall, these communication flows and the whole communication and dissemination activities helped structured the SPARTA Network and build a cohesive community informed of the various results and news happening and able to disseminate the information easily. Such internal communication inside the community and to external stakeholders are an essential part to build a community and while the means to apply them inside SPARTA remained limited they should play an important part in any community building.

3.3 Scientific and technical activities

This section focuses on SPARTA's scientific and technical activities which are comprised of the Roadmap instrument (WP3) and the four SPARTA Programs (WP4-7).

3.3.1 Roadmap instrument

This section is an excerpt of the findings of the Roadmap instrument during the full execution of SPARTA as well as its lessons learnt w.r.t. its governance. The complete report can be found in deliverable D3.5 [SPARTA SRIA Lessons Learned and Future Assessment, PU, M38].

Since the first year of the project, the SPARTA Roadmap development was centred around a mission-oriented approach. The mission defined by the SPARTA Roadmap was to strengthen digital sovereignty, for which SPARTA has taken a technology-driven approach. However, the discussions in the Roadmapping Focus Group (RFG) 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, ELSA aspects,… In this way, various paths to achieve the global goal of digital sovereignty can be identified and included in the Roadmap consolidated through the defined mission as per the mission-oriented approach. This chapter provides a short overview of scope of roadmapping activities and key findings that were considered important to be shared.

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 high quality and comprehensive information integrated into the roadmap. The produced roadmaps could not have been feasible to a single roadmap committee, nor could they have benefited from coherent structure without it. Thus, we believe that such 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. This cooperative model has already been tested in the RFG, coordinated by SPARTA and made of members from the all CCN Pilots, ECSO, and the EC. Recently, the EC provided hints on upcoming roadmapping activities at the ECCC/NCCCs that may benefit from the RFGs' experience, execution process and lessons learnt.

The overall scope and key findings can be summarised as follows:

- SPARTA roadmap prioritizes the scientific challenges that are required for achieving digital sovereignty in the EU. Those challenges are 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.
- We would like to point out that an iterative and agile mission-oriented roadmapping approach is highly advantageous. We therefore recommend that the ability to adapt and be flexible 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 sovereignty has been confirmed. The prioritization of trustworthy, secure hardware, trustworthy data rooms, and trustworthy AI systems highlighted in the roadmap is essential in order to give European companies and state institutes the ability to act independently.
- We strongly recommend giving more priority to the question of developing resilient software and hardware architectures.
- The question of cyber defence 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.
- Information have a decisive influence on opinion-forming and decision-making. 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 and to define common philosophy how cross discipline areas where cyber security meets information security and hybrid threats.
- The SPARTA roadmap mostly focused on identifying technological challenges required to achieve the mission of digital sovereignty. 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. Legal, societal, ethical and economical challenges are a few to be mentioned. Identification of those aspects and reflection on them in the roadmap requires multidisciplinary competencies and extended roadmap structure. For example, we need to incorporate cybersecurity in the various existing business models so that it becomes a part of competitive advantage.
- Complex security is one of the weaknesses in existing CS roadmapping activities. In order to address it comprehensively it should go beyond classic CS and incorporate combinations of different technologies and disciples.
- 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 of cybersecurity measures 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

The roadmap Committee of SPARTA exchanged ideas throughout the project with the other CCN pilots and ECSO. This has proven to be 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 are 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.

3.3.2 Programs

In the following sections, the four SPARTA Programs are discussed through the lens of their governance. Updating on previous findings from D1.1 or D1.3, they report the experiences and lessons learnt during the third year of SPARTA.

3.3.2.1 Program 1: T-SHARK – Full-spectrum cybersecurity awareness

By design, the activities within the T-SHARK program are very collaborative and require significant governance efforts. Their aim is to build and demonstrate the integrated synergies of sub-cases, providing a backbone of comprehensive cybersecurity and laying the background for collaborative comprehensive cybersecurity threats prediction.

During the first year of development, the focus was put on the identification of the added value by individual sub-cases while during the second year, the focus moved from individual, towards integrated actions. For the last year, the goal was to compose the comprehensive structure, where synergy is achieved by information collected from all sub-cases. It allows to demonstrate the comprehensive collaborative cybersecurity concept, even considering limited, and sometimes very specific, scope of all individual sub-cases.

The cooperation dimension within T-SHARK can be described in two dimensions – internal (enhancing synergies) and external (involving activities beyond the program). Internal cooperation was a very important aspect during the second and third year, as individual sub-cases had to demonstrate interconnectivity and align the sharing of information. The information sharing platform developed within the scope of T-SHARK, consists of two technical platforms – Malware Information Sharing Platform (MISP) and Collaborative and Confidential Information Sharing and Analysis for Cyber Protection (C3ISP). This provided functionality to share not only information, available for all partners in eco-system (MISP), but also limited access data (C3ISP). This was more of a technical nature, but also required a lot of dialog, explanations and modifications. In addition, special attention was given for collaborative methods, techniques and policy on data sharing development and cross-institutional as well cross-boarder threats intelligence information exchange.

The need for external cooperation became significant after the first and second years of activities. Nevertheless after involving external stakeholders such as SAPAN during the second year which provided valuable insights, additional efforts to involve external initiatives was not in the focus during the last year of implementation, but rather integration of existing stakeholders needs and perspectives.

Adherence to SPARTA's research governance activities evolution

As governance is one of the focus Tasks within T-SHARK, continued efforts were made to pilot new ways to better describe and guide all Sub-cases.

The previous two years of SPARTA led to search for different models of innovation governance. Thus building on the findings from the previous two years, the main research evolution in T-SHARK can be summarized in defining and piloting few new frameworks:

- TRL, supported by System Readiness Level (SRL) and Manufacturing Readiness Level (MRL) – continue maturation and development progress.
- Continue working on innovation integration framework - facilitates reduction of complexity to ease up-take process.
- How specific outcomes of sub-cases add value to treat intelligence, how they can be connected to each other, and related questions were the focus of last period. In-depth analysis of awareness building process, relevance of information received, developing links between data providers and other issues at a detail level were discussed. No specific instruments were applied, discussions and co-creation were main means of action.

The current state of T-SHARK's research or innovation governance is not at its final point, where final conclusions can be drawn but rather solid lessons learnt and roadmap for future work package.

Interaction with transversal activities

Activities in T-SHARK are closely linked to the development of the Skills Framework within WP9 and several joint activities or workshop have been carried out during the project on these topics with WP9. At the final stage of the project, developing full-spectrum cybersecurity threat intelligence methodology, the link with WP9 became even more relevant. Analysis of threat intelligence relevant skills was based on the D9.1 (providing framework) and D9.2 (providing curricular descriptions). The use of already documented analysis allowed to identify relevant skills and evaluate availability of such skills for cybersecurity students.

Friendly coopetition

Stage Gates methodology applied in T-SHARK Program (see T-SHARK deliverables for more explanation) is of the competitive nature by design. Nevertheless in the later stages of T-SHARK, the application of Stage Gates methodology moved from a competitive nature to more of a co-development mode. Indeed as T-SHARK moved to build a comprehensive and well integrated pictures with all Sub-cases the need to understand other sub-cases and their relation were very meaningful to create joint results.

The integration phases have showed that it is highly important to have well defined use cases as basis for overall collaborative process organization and governance in order to link and integrate highly diverse maturity level innovative solutions.

Research focusing mechanisms

In T-SHARK, technical teams are left with a wide autonomy on the organization of implementation activities. The core goal of all of the teams efforts is to produce a final and international integrated method and organisation combing technical, societal, legal and methodological innovations into one solution. a final integrated method is the core goal of common efforts.

During the course of the project, it was identified that international alignment aspects demands for extra efforts and going through the second year of program implementation showed that for such a wide-scale research program, where an efficient collaboration structure is crucial, the pandemic lockdown definitely had an impact and showed how important are periodic physical meetings. It is, however, hard to assess how the implementation would be different under different circumstances.

Moving towards integrated framework, methodology and solution have showed clear difference between research governance and innovation governance. These two processes overlap, however are not the same. Still to highlight, - research process is rather niche problem (challenge, opportunity) oriented and innovation requires more holistic and multidisciplinary approach.

Time horizon

Individual T-SHARK technical innovations are focused on concrete challenges identified in current cybersecurity operational environments. High maturity innovations are made available for operational use.

At the same time, the development of a cybersecurity threat prediction methodology is a long-term research topic, addressing global cybersecurity trends and focusing on mid to long term perspectives for adoption and implementation.

T- SHARK has been introduced to regional consortiums, and while considering potential uptake possibilities it is showed necessity for wide scale promotion in order to have core aspects identified for cross-boarder uptake roadmap creation.

Societal and ethical perspectives

The T- SHARK research program has addressed societal, legal and ethical perspectives in its design. From the three mega challenges on ELSA aspects identified in year 1 and research in year 2, T-SHARK performed research and in-depth analysis including information gathered from 18 MS. In parallel, a legal assessment for each individual technical subcase development has been conducted, serving as major input to the integrated techno-societal innovation development.

Additionally, to fully integrate these aspects in the stage gate process, the evaluation of sub-cases is not only using TRL but also on different SRL criteria that provide comprehensive views on innovation development.

Enabling partnerships in research governance

The activities around T-SHARK Arbitrage Group have been continued during the third year of SPARTA and we reciprocate here the findings from D1.3, that this approach of enabling partnership is valuable. Nevertheless and while specific benefits for AG members are proposed, there must be more efforts allocated to develop and keep the AG as a community. It would also be useful to discuss possibilities to construct an AG type of body, able to get involved in different EU projects research governance.

3.3.2.2 Program 2: CAPE – Continuous assessment in polymorphous environments

Adherence to SPARTA's research governance activities evolution

Technical activities are carried out in the four tasks of CAPE demonstrating complementarity and integration of the tools with the help of CAPE's flexible yet redundant governance model. Through bi-weekly task meetings, monthly WP meetings and easy delegation through experts tasks and WP leader, the governance model has matured to maximizes interactions with the program and to produce quality results from the contributions of the different partners.

Interaction with transversal activities

As detailed in deliverables D5.4 and D11.5, the policy activities inside CAPE related to certification were smoothly handled by integrating WP11 partners at task level in CAPE's activity.

Friendly coopetition

With a cooperative mode of management inside CAPE and close assessment targets, CAPE has managed to harmonised the different specification of the tools to produce complementary results. The focus in CAPE was on synergies and competencies between researchers. In turn this governance choice allowed CAPE to showcase elaborate advanced research platforms to showcase its two verticals.

Research focusing mechanisms

Overall, CAPE offers a concrete materialization of cybersecurity and safety assessment and validation in two concrete examples. In terms of governance, deliverables D5.2 and D5.3 provided an example of the collaboration for an integrated research and validation workflow in CAPE, with validation as an equality important part of the workflow which is often expensive for individual researchers. The mutual exchange and joint elaboration of validation tools and processes is thus an important lesson-learnt from CAPE. Deliverable D5.4 amplifies this collaboration, not only from a writing perspective, but also from a technical perspective, as integration of tools into the use case development environments required close collaboration between all partners.

In a nutshell, the major research-focusing mechanism in CAPE has been the development of use cases accessible to all project participants, with a sufficiently broad scope and sufficiently easy access that anyone could easily participate. In addition, a few of the tools developed have cross-cutting capabilities that are demonstrated in a stand-alone manner. Additionally, CAPE has produced a dataset, available upon request, to stimulate the cybersecurity research community related to malware.

Time horizon

There are two extremely different time horizons in CAPE related to both vertical of the program. As detailed in D1.3, vertical 2's tools is extremely close to being usable by anyone or has already been opened and made available to the community while what is done in vertical 1 will only bear fruits after the end of the project due to the difficult compromise between security and safety.

Societal and ethical perspectives

In CAPE, in addition of the global goal to increase trust in digital services, the link with ELSA is made through certification activities to address the legal and regulatory framework. Insurance as another ELSA aspect also plays an important role in CAPE in case of failure or new vulnerabilities.

Additionally, CAPE is demonstrating "certification in action", with the capability to certify two mechanisms (platooning and single-sign-on) on two different use cases, against realistic threat models. This also furthers the development of certification schemes, through the development of publicly available certification profiles.

Enabling partnerships in research governance

CAPE has successfully engaged a wider community, due to the inclusion of some tools in open platforms, and typically the ECLIPSE platform for at least three of our tools at the time of this writing. This availability of tools impacts the wider computer science community.

Additionally, many tools are freely available over GitHub, or available upon request. The malicious packages dataset is available upon request. Most of the tools are supported by companies and RTOs, ensuring sustainability beyond the program's end.

Governing research outputs

Building on the key points and take-ways already mentioned in deliverable D1.3, the third year of the program, more oriented on results' finalisation, and publication adds another key finding and recommendations on the CAPE governance takeways:

- Publication of research results, not only papers but tools and datasets, enhances dissemination, confirming the principle of open science. The "upon request" availability does not preclude dissemination, but rather ensures proper credit to the creator of the tool or dataset, and stimulate community interaction.
    - Recommendation for further CCN: provide support for one or several hubs enabling sharing of tools and datasets, with credits to the creators.

3.3.2.3 Program 3: HAII-T – High-Assurance Intelligent Infrastructure Toolkit

HAII-T program activities require a strong and continuous interaction among the involved partners. Although each task has specific objectives, the overall goal is to express the full potential of the synergy of the technologies contributing to the toolkit.

Since Year 1, a single, shared environment for staging the program demonstrations and for driving the integration process has been a priority. Hence, a unified case study where each partner contributes with a dedicated application scenario was developed. The unified use case was an asset and one of governance instruments for fostering both internal and external interactions, ensuring continuous integrity and mission oriented agile research and development. Throughout all 3 years of the implementation it allowed to have manageable and timely diverse activities organization, despite Covid-19 have made huge impact on the plans, especially in the means of synchronization, coordination, alignment and communication.

Although central, the use case is not the only governance instrument of HAII-T.

Adherence to SPARTA's research governance activities evolution

In the first year, the reference model for the security-by-design framework was developed in HAII-T and implemented as in a first version of the HAII-T demonstrator in Year 2. All these activities required a continuous interaction among the expert partners. Finally, Year 3 was mostly focused on fine-tuning of deliverables individually and ensuring best integration to work as comprehensive solution delivering complete realization of the use case.

A collaborative view was taken in terms of governance, mixing individual contribution and global integration through mixing selected application scenario in a well-integrated unified use case. This approach allowed every partner to share its own expertise and to learn from others by collecting

feedback and integrating with them. This also allowed to successfully build a comprehensive framework and a unified use case.

Interaction with transversal activities

In addition of the continuation of collaboration with training activities, the interaction with certification aspects (WP11) and HAII-T were successfully extended with T6.5 on GDPR compliance and other standards for IoT during the third year of SPARTA. This work on a key priority for the future certification frameworks in IoT cybersecurity is detailed in D6.4 and D11.5.

Finally, the results of HAII-T finalised in Year 3 with a demonstrator and its associated virtual environment have been integrated in the SPARTA JCCI platforms to foster interaction and allow a greater part of the community to access it.

Friendly coopetition

HAII-T mainly follows a collaborative approach as suggested previously. The goal in HAII-T is to construct a unified framework and use case built from the construction integration of the various tools. This resulted during the whole duration of the project in joint publications from WP6 partners, in particular with a joint paper describing the application scenarios of the project.

This collaborative approach was also extended to external partners, with the DIOT srl which joined the SPARTA Friends program during the second year. As an innovative start up in smart home environments, they applied the HAII-T toolkit and framework for the security assessment of their products. This work was delivered and demonstrated in the third year of SPARTA.

Research focusing mechanisms

WP6 activities focus on intelligent infrastructures. These infrastructures can have different sizes and belong to different kinds of organization, from small, e.g., smart homes, to large scale, e.g., critical infrastructures and smart industries. After agreeing on it in the second year, the unified use case was finalized and delivered during Year 3, driving overall integration process and proving to be a strategic asset for the entire WP and for SPARTA in general.

Time horizon

HAII-T deals with existing problems in the security of smart environments through its unified use case and the activities carried out in defined virtual environment, which has designed by including technologies and components for the real world. While in a virtual environment, the activities carried out in the project are expected to be able to be readily ported to real infrastructures.

Societal and ethical perspectives

From year 2 onwards, WP6 started regular interaction with WP2 on identifying ELSA-related topics in HAII-T. The privacy issues received major attention in that regard and a concrete study of privacy-related issues for the whole WP6 was delivered in D6.4 at the end of the project, some of which were demonstrated in the unified use case.

Enabling partnerships in research governance

The developed demonstrator relies on two strategic assets, i.e., the virtual infrastructure and the application scenarios contributing to the unified use case. These represent a valuable resource that during Year 3 was packed and released to the community. The presentation of these assets to the public and different communities occurred through publications, deliverables and code repositories, detailing the different case studies under the unified use case developed in the project.

Governing research outputs

HAII-T provides a contribution to the community of smart infrastructures designers and developers. In particular, demonstrators should include privacy and security by design and assessment for the intelligent infrastructures which both public and private stakeholders are pushing. In that sense, with the work validated and demonstrated in the project, HAII-T aims to strongly support the security evaluation and certification of intelligent infrastructures.

3.3.2.4 Program 4: SAFAIR – Secure and Reliable AI Systems for Citizen

Adherence to SPARTA's research governance activities evolution

SAFAIR was focused on the flexibility of the governance activities. Level and quality of interactions between the programme contributors allowed to implement participative coordination and management approach in SAFAIR. The program was composed of research and development activities related to threat analysis (mainly in T7.1), technical specification and development of defensive and reactive mechanisms, mechanisms enhanced explainability and fairness of Artificial Intelligence (AI) systems, and activities related to validation and evaluation of developed solutions. Teleconferences/online meetings were organized monthly at programme- and ad-hoc at the task-level.

Interaction with transversal activities

SAFAIR actively interacted with transversal SPARTA efforts, in particular contributing to the raising cybersecurity awareness, sustainable exploitation of results, and dissemination and communication activities.

Friendly coopetition

SAFAIR program promoted friendly coopetition in the area of secure and reliable AI systems by launching the SAFAIR adversarial AI contest. It aimed to evaluate the robustness of defence techniques proposed by participants. This encouraged the creation of deep learning models which are robust to a variety of attack methods. The plan and proposal of the contest were described in D7.3, the announcement and contest rules were published in February 2021, while the deadline for the final submission was set on June 2021. Evaluation of the competition and final results of the contest were reported in D7.6.

Research focusing mechanisms

Key research focusing mechanisms applied in the SAFAIR were collaboration and emphasis on multidisciplinary. Research on societal and ethical perspective of AI usage required a broad analysis of not only technical, but also organizational, societal, ethical and legal dimension of artificial intelligence.

Time horizon

The initial efforts of the SAFAIR were oriented on enabling future secure and reliable AI systems. Therefore, the T7.1 work was oriented towards aiding in the identification of potential security and privacy incidents that may occur to AI systems and attacks against AI components in systems that need to be defended. As current taxonomies, attacks, systems and techniques classifications and identified emerging trends in securing AI systems will be valid in the future, the time horizon of this part of the research can be described as mid- to long-term.

For the technical tools developed in the SAFAIR, as reported in D7.5, though the proposed methods have their drawbacks, the benefits they offer outweigh the costs. Many of the methods are flexible, model-independent, simple, easy to understand, and their proper usage allows to defend the model or gain insights into the model. Therefore, they will remain a valid proposition in the foreseeable future.

Societal and ethical perspectives

Legal, societal and ethical aspects were inherent perspectives build in the SAFAIR research and development. Tasks T7.3 (Enhance explainability of AI) and T7.4 (Design measures for fairness in AI) and their results directly address ethical and societal issues related to use of AI systems. Explainability of more and more popular services based on AI mechanisms is crucial for increasing transparency, social understanding and finally confidence in relation to Artificial Intelligence. On the other hand, improvement on AI-based decision making in e.g. public services will contribute to citizens' security. As for fairness aspects, design measures for improved fairness in AI proposed in the SAFAIR are focused on reducing conscious or unconscious bias in decisions made by AI,

therefore contribute to one of ethical imperatives recognised by the High-level Expert Group on Artificial Intelligence.

Enabling partnerships in research governance

SAFAIR successfully engaged and encouraged contribution of a wider community to the research in the field of adversarial AI, by launching its adversarial AI contest which results and organisation are described in D7.6 – Final version of evaluation and validation plan.

Governing research outputs

The key research output of WP7 SAFAIR programme is the final demonstrator covering three of the identified AI-related challenges: security and robustness, explainability and fairness. As for security and robustness field, we implemented several attacks and defence mechanisms, we proposed defensive methods against evasion attacks. SAFAIR also organized a contest to evaluate some evasion attacks and the defence strategies adopted by the participants.

Concerning explainability and fairness, we presented a novel approach based on surrogate model explainability and a component based on ShapKit, a Python module dedicated to local explanation of machine learning models.

Another research output is SAFAIR AI Threat model and Knowledge Base of SPARTA extended and improved during the SPARTA to take into account emerging results from ENISA and other relevant initiatives on AI threat landscape.

Finally, we presented the legal aspects of AI, a practical checklist for software developers in order to respect the equity criteria throughout the development process.

Chapter 4 Becoming a sustainable CCN

4.1 Job description

Following the modular governance framework introduction in D1.3 (Improving a CCN pilot, PU, M24), a portfolio of job descriptions corresponding to the SPARTA main roles is developed hereunder. This provides a consistent management-level view of the skills and characteristics needed to operate a cybersecurity competence network.

The goal is to provide a portfolio of roles which would be useful for an operational CCN aiming to concretize the ECCC+NCC funding actions by establishing a structure designed at boosting their performance and impact. All roles, except the Program Leader one, are meant to be filled only once, at network-level to support all the Programs deployed. The choice of stating the capacities expected to operate a Network around its leadership has been made to increase its actionability and be in line with SPARTA's third governing principle : Create opportunities for open leadership [Bootstrapping a CCN Pilot, PU, M12].

We keep the SPARTA structure of transversal activities (responsibility, roadmap, partnership, education / training / awareness, sustainability / exploitation, certification, and communication / dissemination, management) and technical programs. The governance activity, prominent in SPARTA, is not kept as it is for a sustainable network as it was mainly used to build and experiment governance aspects in the pilot while it is expected that the full-fledge network will have a fixed – though dynamic – governance.

The job descriptions presented in this report are based on the ENISA ECSF [4], built from the activities carried out by the ENISA European Cybersecurity Skills Framework ad-hoc working, to which SPARTA has been appointed as an observer. They encompass the experience of SPARTA activities and programs leaders after the execution of the pilot.

4.1.1 Responsibility Leader[2]

Profile Title	Responsibility Leader
Alternative Title(s) *Lists titles under the same profile*	Ethics Manager Value Lead
Summary statement *Indicates the main purpose of the profile.*	The Responsibility Leader is the person assigned to coordinate and conduct tasks related to ethical values elicitation and prioritization and traceability of values through the requirements and design artifacts throughout the Programs covered by the Network.
Mission *Describes the rationale of the profile.*	The Responsibility Manager focuses on the identification, analysis, and prioritization of ethical values and their incorporation in the system design. S/he is not "the person in charge of ethics" but contributes subject matter expertise and facilitative skills, bridging gaps between engineering, management, and ethical values in a constructive way.

[2] Adapted from [2].

Profile Title	Responsibility Leader
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	Ethics and Social Readiness Policy
Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*	a) Organize, analyse, communicate, and record ethical and/or value related concepts, concerns, activities and decisions in a project b) Facilitate discussions and value-related activities to accompany a project in its design efforts c) Build compromises through practices like participatory design d) Record decisions and those who are accountable in a consistent and as easily retrievable form, e) Track and report related decisions to adhere to transparency f) Maintain the Case for Ethics Tasks d) to f) supports the communication of technical decisions and system functions to stakeholders through the Management leader.
Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	a) to communicate with all stakeholders in an adequate and sensitive manner to design solutions that are acceptable to all b) sense what is desired and to consistently deliver high quality to the satisfaction of stakeholders c) to achieve the goals and strive for improvement or excellence d) Sharing appropriate behaviours, such as teamwork, leadership, and compliance with professional codes e) to adapt to changing circumstances and demands by creating new know-how f) to perform the requisite tasks efficiently
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level) Basic Understanding of: Understanding of: Knowledge of: Advanced knowledge of:*	a) Ethics and governance of science and technology b) Data protection and compliance c) Risk management d) Deliberations methods and strategies e) Participatory methods in systems design and assessment f) Understanding of the multidiscipline aspect of cybersecurity g) Technical domain knowledge: empirical, academic, or a blend of both • Knowledge of cybersecurity frameworks, policies, regulations, legislations, certifications, and best practices • Knowledge of cybersecurity strategic objectives, goal, and roadmap

Profile Title	Responsibility Leader	
	h) The experience of application (knowing what works) in different contexts and the requisite skills i) Conflict resolution practices	
e-Competences **(from e-CF)** *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	A.3. Business Plan Development A.7. Technology Trend Monitoring A.10. User Experience D.11. Needs Identification E.3. Risk Management E.4. Relationship Management E.9. Information Systems Governance	Level 3 Level 3 Level 4 Level 5 Level 4 Level 3 Level 5

4.1.2 Roadmap Leader

Profile Title	Roadmap Leader
Alternative Title(s) *Lists titles under the same profile*	Cybersecurity Strategic R&I Roadmap Manager/Director/Coordinator/Officer Head of Strategic R&I Agenda
Summary statement *Indicates the main purpose of the profile.*	Coordinates the processes and activities of establishing and maintaining a short- to long-term roadmap for cybersecurity research and innovation aligned with the overarching mission of the consortium, including identifying strategic priorities of current and emerging challenges in cybersecurity, by consolidating and integrating expert input from the network of R&I programmes and roadmap stakeholders.
Mission *Describes the rationale of the profile.*	In order to use funding in a targeted manner and with the greatest possible impact, it is necessary to systematically develop research and development agendas for short, mid and long-term periods. This must be geared towards a visionary mission that will last for many years and that must be developed together with all relevant stakeholders. In order to implement the mission, prioritization must be coordinated and sub-goals defined together. In order to fulfil this task, the skills of a research manager and research coordinator are required, with the competence to think ahead in a visionary way, but at the same time to design the implementation in concrete terms and to involve all relevant stakeholders in the processes in a goal-oriented manner.

Profile Title	Roadmap Leader
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• - Cybersecurity Strategic R&I Roadmap

Main task(s)
A list of typical tasks performed by the profile.
 	
is tasked to:
	• Adaptation, synchronization, progress measurement, and improvement for governance of R&I activities
	• Defines, implements, and maintains governance framework within the roadmapping department
	• Coordinate and facilitate regular network-wide exercises and workshops for:
	  ○ Establishing overarching mission statement of the roadmap
	  ○ Identifying seed challenges and emerging topics for the roadamp
	  ○ Constantly updating and upgrading the existing roadmap challenges, by consolidating and integrating the collected input in the roadmap
	  ○ Deriving a prioritization of roadmap challenges
	  ○ Updating the prioritization of roadmap challenges
	• Scan horizon and compare with other established roadmaps at EU-level, national-level, pilot-level, community-level
	• Measure roadmap impact by identifying number of tender calls and funded projects aligned with the roadmap at EU and national level

Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	• ability to communicate to a large variety of people • ability to transfer technology research to industry and/or governmental institutions • ability to collaborate and to achieve compromises in situations when several different viewpoints have to be taken into account • excellent abilities to assess the importance and level of disruptiveness of new technological developments • excellent interdisciplinary skills to be able to cover not only technological aspects, but also social, economic and legal ones in a balanced manner • ability to understand knowledge of business needs, ability to address their needs (speaking their ‘language’, i.e. to explain innovations in terms of value-add • ability to develop ambitious visions • an excellent scientific track record in fundamental and applied research • long-standing experience with research management • long-standing experience in agenda setting for political and governmental bodies • - a broad network of international experts: scientific but

Profile Title	Roadmap Leader
	also industrial, governmental, etc.
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level) Basic Understanding of: Understanding of: Knowledge of: Advanced knowledge of:*	• Advanced understanding of the topics the roadmap should cover • Advanced knowledge of technological, as well as economic developments • Advanced experience and knowledge in fundamental and applied research and development • Advanced knowledge in agenda setting for political and governmental bodies • Advanced knowledge in identifying emerging research and technology fields • Advanced knowledge in leading interdisciplinary teams
e-Competences **(from e-CF)** *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	No additional competences, everything has already been mentioned in the bullet pints above

4.1.3 Partnership Leader

Profile Title	Partnership Leader
Alternative Title(s) *Lists titles under the same profile*	Cybersecurity ecosystems manager Cyber security community coordinator
Summary statement *Indicates the main purpose of the profile.*	Manages a network of organizations and promote cooperation on research and innovation activities of mutual interest for the stakeholders in the partnership.
Mission *Describes the rationale of the profile.*	Defines, maintains and communicates the cybersecurity community, vision, strategy, policies and procedures. Manages the coordination and synergies of implementation of the cybersecurity activities across the organisations. Assures information exchange with all the stakeholders and different ecosystems related to cyber security.
Deliverable(s) *Illuminate the Profiles and explains relevance*	• Cybersecurity partnerships • Cybersecurity ecosystems

Profile Title	Partnership Leader
including the perspective from a non-Cybersecurity/ ICT point of view.	
Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*	• Define, implement, communicate and maintain a cybersecurity partnership among several stakeholders in order to promote the cyber security in the interest of the involved parties with initiatives that exploits the synergies in the partnership. • Prepare and present cybersecurity vision, strategies and policies for approval by the senior management of the organisations involved and ensure their execution. • Supervise the application and improvement of the joint initiatives program (JIP) • Develop plans for the growth of the partnership • Develop relationships with cybersecurity-related authorities and communities • Develops the organization of events for increasing the cooperation among stakeholders • Secure resources to implement the joint initiatives program • Review, plan and allocate appropriate resources • Promote the growth of cyber security culture in all the relevant stakeholders
Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	• Communication and strategic vision capabilities for cyber security • Understand core organisational business processes and relationships among stakeholders in cyber security • Analyse and implement cybersecurity standards, frameworks, policies, regulations, legislations, certifications and best practices • Manage cybersecurity incentives for cooperation and value chain in cyber security • Develop, champion and lead the execution of a cybersecurity strategy in multi-stakeholders ecosystems • Understand core multi-organisational, cross-organizational, cross-border business processes • Influence the diversity an inclusiveness in the cybersecurity culture of involved stakeholders • Ability to lead constructive conflict resolution to align and synchronize for strategic objectives implementation.
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.*	• Knowledge of cyber security ecosystems at international, national and regional level • Knowledge of cybersecurity tactics, techniques and procedures • Knowledge of the relevant stakeholders in the community

Profile Title	Partnership Leader	
(Depending on the level) Basic Understanding of: Understanding of: Knowledge of: Advanced knowledge of:	• Knowledge of cybersecurity and privacy standards, frameworks, policies, regulations, legislations, certifications and best practices • Understanding of ethical cybersecurity organisation requirements • Knowledge of management practices • Knowledge of risk management frameworks • Knowledge of conflict resolution practices	
e-Competences (from e-CF) *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	A.1. IS and Business Strategy Alignment	Level 5
	A.7. Technology Trend Monitoring	Level 5
	A.9. Innovating (not on products but on management)	Level 4
	C.4. Problem Management	Level 4
	D.8. Contract Management	Level 4
	D.1. Information Security Strategy Development	Level 4
	D.10. Information and Knowledge Management	Level 4
	D.11. Needs Identification	Level 4
	E.1. Forecast Development	Level 4
	E.2. Project and Portfolio Management	Level 4
	E.4. Relationship Management	Level 5
	E.7. Business Change Management	Level 5

4.1.4 Education, Training and Awareness Leader

Profile Title	Education, Training and Awareness Leader
Alternative Title(s) *Lists titles under the same profile*	Education, Training and Awareness Officer Education, Training and Awareness Manager Head of Education, Training and Awareness
Summary statement *Indicates the main purpose of the profile.*	Plans, manages and coordinates the cybersecurity education, training and awareness activities. Prepares, executes and evaluates education, training and/or awareness campaigns, designs and maintains education strategies and supervise their application at education and training providers. Monitors new trends on the job market and implements necessary updates of education and training programs.

Profile Title	Education, Training and Awareness Leader
Mission *Describes the rationale of the profile.*	Oversees and coordinates the activities of education and training providers on a higher level. Steers the activities in the education sector. Connects academia, professional training institutions, industry and government.
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	Education and training strategies Good-practice education and training curricula Cybersecurity skills frameworks Education and training plans Accreditation and endorsement rules Training and education status reports
Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*	Analysis of existing cybersecurity programs, courses, subjects Creation of skills frameworks Creation of guidelines for education, training and awareness Creation of accreditation and endorsement programs Organisation and coordination of the community Finding new approaches for education, training and awareness-raising
Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	Analyse and implement cybersecurity standards, frameworks, policies, regulations, legislations, certifications, and best practices Communicate, coordinate, and cooperate with internal and external stakeholders Apply relevant standards, best practices, and legal requirements for cybersecurity Understand core multi-organisational, cross-organizational, cross-border processes Lead constructive conflict resolution to align and synchronize for strategic objectives implementation Identify needs in cybersecurity awareness, training and education Develop evaluation programs for the awareness, training and education activities Identify and select appropriate pedagogical approaches for the intended audience Motivate and incentivise learners
Key knowledge *A list of essential knowledge required to perform work functions and*	Understanding of the multidiscipline aspect of cybersecurity Knowledge of pedagogical methods Advanced knowledge of cybersecurity awareness, education and training programme development

Profile Title	Education, Training and Awareness Leader	
duties by the profile. *(Depending on the level) Basic Understanding of: Understanding of: Knowledge of: Advanced knowledge of:*	Advanced knowledge of professional training certifications Advanced knowledge of cybersecurity-related legal framework, regulations, standards Advanced knowledge of cybersecurity frameworks, methodologies, controls and best practices Advanced knowledge of accreditation processes Advanced knowledge of education strategies and guidelines Knowledge of a job market	
e-Competences **(from e-CF)** *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	D.3. Education and Training Provision D.9. Personnel Development E.8. Information Security Management	Level 3 Level 3 Level 3

4.1.5 Sustainability and Exploitation Leader

Profile Title	Sustainability and Exploitation Leader
Alternative Title(s) *Lists titles under the same profile*	Sustainability and Exploitation Officer Sustainable Exploitation Manager Head of Sustainable Exploitation
Summary statement *Indicates the main purpose of the profile.*	Supports researchers and innovators in transforming their ideas or research outcomes into sustainable solutions or products Identifies market or ecosystems gaps, which would benefit from ongoing or foreseen research and innovation activities Coordinates with relevant organisations (Incubators, Technology Transfer Offices, Innovation hubs, etc.) to facilitate the creation of start-ups or equivalent initiatives based on the research products or outcomes.
Mission *Describes the rationale of the profile.*	Leads and coordinates activities allowing to transform the Research and Innovation outcomes into sustainable solutions or products. Drives cooperation and collaboration between industry, research, innovation hubs and the ecosystem at large. Conducts exploratory work on tools and methods to facilitate the creation of sustainable solutions and products from Research and Innovation activities.

Profile Title	Sustainability and Exploitation Leader
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	Sustainable exploitation planning Sustainable exploitation toolbox Cybersecurity market gaps analysis Contribution to strategic roadmapping for cybersecurity R&D in the perspective of emerging or identified market needs Support to matchmaking between possible partners for the development and exploitation of sustainable solutions or products Sustainable exploitation analysis reports
Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*	Analysis of existing solutions and products categories on the market Gap analysis of existing offers on the market and identification of needs Creation of documentation / guidelines on how to identify the most appropriate sustainable exploitation strategy for a given solution or product Creation of tools and platforms facilitating the emergence of exploitation opportunities for members of the Community engaged into innovation or research Coordination with research and innovation supporting organisations or initiatives, to the benefit of the Community actors engaged in research or innovation Contribution to the ECCC strategic roadmapping effort
Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	Understand generic security domains and map products and services into these domains Knows and understand cybersecurity best practices, standards, frameworks, certifications, policies, regulations, and legislations Identify and document needs and gaps on the market of cybersecurity solutions and products Motivate and incentivise Community members eager to develop solutions and products based on research and innovation outcomes Help to evaluate the maturity, quality, effectiveness and relevance of proposed solutions and products Communicate, coordinate and cooperate with external stakeholders Manage or support cross-functional, cross-organisational, cross-border projects and initiatives Support Community members in constructively solving possible conflicts, in particular with regards to business model design and Intellectual Property management

Profile Title	Sustainability and Exploitation Leader	
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level) Basic Understanding of: Understanding of: Knowledge of: Advanced knowledge of:*	Understanding of the different dimensions of cybersecurity Understanding of Intellectual Property challenges and possibilities, including Open Source ones Knowledge of the national cybersecurity ecosystem, community and market Knowledge of Business Models design Knowledge of innovation supporting frameworks and institutions Knowledge of Technology Maturity assessment frameworks and methods Advanced knowledge of cybersecurity standards, regulatory and legal frameworks Advanced knowledge of European initiatives supporting cybersecurity industry development	
e-Competences **(from e-CF)** *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	A.1. IS and Business Strategy Alignment A.3. Business Plan Development A.9. Innovating D.10. Information and Knowledge Management D.11. Needs Identification E.7. Business Change Management	

4.1.6 Certification Leader

Profile Title	Certification Leader
Alternative Title(s) *Lists titles under the same profile*	Cybersecurity Certification Manager Cybersecurity Certification Director Cybersecurity Certification Officer Head of Certification
Summary statement *Indicates the main purpose of the profile.*	Leads and manages the cybersecurity certification policy. Defines the cybersecurity certification strategy and manages research and experimentation with the research programs. The main objective is to align certification support activities with the different European and different national cybersecurity certification initiatives. This will be achieved with the following sub-objectives: • Mapping international/European cybersecurity certification initiatives and the Cybersecurity Act certification framework

Profile Title	Certification Leader
	• Liaising with European and national cybersecurity authorities • Supporting European and national cybersecurity authorities with evaluation facilities capable of evaluating cybersecurity act certification schemes • Providing recommendations for software development process cybersecurity compliance
Mission *Describes the rationale of the profile.*	Defines the cybersecurity certification strategy, defines the research and validation across the research programs. Embeds proactive certification initiatives by assessing, informing, alerting and educating the entire network about certification. The mission includes the following tasks: • Monitoring and analysis of international and European cybersecurity certification. • Liaison with European and national cybersecurity authorities. This task aims to create and maintain communication channels with national cybersecurity authorities. • Cybersecurity evaluation facilities. This task aims to make cybersecurity evaluation facilities available with support for cybersecurity act certification schemes. • Process oriented certification concepts for complex mainstream commercial software systems. This task aims at defining process-oriented certification concepts for complex mainstream commercial software systems.
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	Cybersecurity certification policy Cybersecurity certification strategy Cybersecurity certification strategy implementation plan and report Cybersecurity Roadmap and report International and national cybersecurity certification initiatives report Cybersecurity compliant development processes report, Cybersecurity evaluation facilities report Report on liaison with national cybersecurity authorities
Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*	• Mapping of international and European cybersecurity certification. This task aims to analyse different national European cybersecurity initiatives as well as international efforts. The analysis will also take into account the EU Cybersecurity Certification Framework. • Liaison with European and national cybersecurity authorities. This task aims to create and maintain communication channels with national cybersecurity authorities. • Cybersecurity evaluation facilities. This task aims to

Profile Title	Certification Leader
	support cybersecurity evaluation facilities to plan to support the latest versions of cybersecurity certification schemes, and to make their evaluation processes more flexible. It also aims at collecting data about the certification process to analyse it and make evaluation process improvements. • Process oriented certification concepts for complex mainstream commercial software systems. This task involves defining process-oriented certification concepts for complex mainstream commercial software systems. The aim is to prepare software products for cybersecurity certification as much as possible during the design phase (cybersecurity certification by design).
Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	• Analyse and implement cybersecurity standards, frameworks, policies, regulations, legislations, certifications, and best practices • Communicate, coordinate, and cooperate with internal and external stakeholders • Apply relevant standards, best practices, and legal requirements for cybersecurity certification • Ability to lead multidisciplinary innovation development and management teams. • Develop, champion, and lead the execution of a cybersecurity certification strategy • Understand core multi-organisational, cross-organizational, cross-border business processes • Ability to lead constructive conflict resolution to align and synchronize for strategic objectives implementation.
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level) Basic Understanding of: Understanding of: Knowledge of: Advanced knowledge of:*	• Knowledge of cybersecurity frameworks, policies, regulations, legislations, certifications, and best practices • Knowledge of cybersecurity strategic objectives, goal, and roadmap • Knowledge of programs and grants • Knowledge of governance and management practices • Knowledge of project management and budgeting • Knowledge of research, development, and innovation (RDI) relevant to cybersecurity certification • Knowledge of resource management • Knowledge of risk management frameworks • Knowledge of conflict resolution practices • Knowledge of cybersecurity tactics, techniques, and procedures • Knowledge of cybersecurity methods, methodologies, tools, and techniques • Understanding of copyright and intellectual property rights issues, standards, and patent filing • Understanding of the multidiscipline aspect of

Profile Title	Certification Leader	
	cybersecurity • Knowledge of future cybersecurity threats, trends, needs and challenges in the organisation	
e-Competences **(from e-CF)** *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	• Plan • A.7. Technology Trend Monitoring	Level 3-5
	• Enable • D.1. Information Security Strategy Development	Level 4-5
	• Manage • E.3. Risk Management	Level 2-4
	• E.8. Information Security Management	Level 2-4
	E.9. Information Systems Governance	Level 4-5

4.1.7 Communication and Dissemination Leader

Profile Title	Communication and Dissemination Leader
Alternative Title(s) *Lists titles under the same profile*	Cybersecurity Communication and Dissemination Manager Content Creator and Social Media manager Cybersecurity Communication and Dissemination Officer
Summary statement *Indicates the main purpose of the profile.*	Develops and implements dissemination and communication strategies to firstly convey cybersecurity R&I activities and results to stakeholders and secondly to create awareness to citizens. Responsible for planning, coordinating and executing dissemination and communication activities. Ensures that the cybersecurity R&I activities are duly communicated to stakeholder's trough, promoting engagement and community building. A Cybersecurity Communication and Dissemination Manager has a social responsibility to work towards pressing issues related to the topic (ex.: gender and diversity gap in cybersecurity) through communication campaigns and specific dedicated activities.
Mission *Describes the rationale of the profile.*	Raise awareness on the research results among selected targeted groups, and build their engagement with projects' objectives, values and mission.

	This is done through the preparation and implementation of a detailed strategy plan, which includes the identification and characterisation of target groups, identification of key messages per target groups; the creation and deployment of communication and dissemination materials (visual identity, logo, templates, posters, social media content, podcasts, newsletters press releases, etc.) and channels (official website, social media accounts, relations with traditional media, etc.); preparation of dissemination and communication events (talks, conferences, exhibitions, scientific events, etc.) both public – for the defined target groups – and internal – for the team; the monitorisation of the planned strategy, timely updates whenever necessary and the evaluation of the communication and dissemination strategy plan.
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• Cybersecurity dissemination and communication plan, updates, and evaluation • Internal and external IT communication infrastructure, website and social media

Main task(s)
A list of typical tasks performed by the profile.
 	
is tasked to:
	• Definition, implementation, monitoring of the dissemination and communication strategy plan;
	• Updates of the dissemination and communication plan, along with an evaluation of the results achieved, lessons learned and produced impact.
	• Promotion of a consistent internal communication, ensuring transfer of knowledge and engagement.
	• Promotion of a consistent external communication, ensuring stakeholders engagement with and understating of the Cybersecurity R&I Programmes and Roadmap related activities and results.
	  • Official website set-up (and maintained) to convey a harmonised view of the progress (including general information, news, scientific publications, information about conferences/ workshops, etc.) and to supply information to stakeholders.
	  • A mailing list (ML) offered to get information.
	  • Organisation of and participation at forums, conferences, talks, scientific and business led events
	  • Design and production of dissemination material to support the visibility of the Cybersecurity R&I Programmes and Roadmap related activities and results.
	  • Design and production of an identity band to provide a strong basis on which dissemination messages capitalise.
	  • Clear and to-the-point presentation of major achievements, events and initiatives, supported by tailored communication materials (podcasts, newsletters, videos, scientific publications, etc.)

Key skill(s)	• Develop, implement and evaluate a communication and dissemination strategic plan

A list of abilities to perform work functions and duties by the profile. *Ability to:*	• Select and characterize target groups/ stakeholders • Analyse and understand the cybersecurity informational needs of each target group • Select the appropriate communication and dissemination channels • Develop a tailored visual identity that matches the values and goals of the organisation • Build and maintain regular communication with colleagues and stakeholders • Understanding stakeholders' different contexts and perspectives, creating empathy • Facilitate multi-disciplinary team collaboration • Promote stakeholders' engagement and participation • Timely reactivity to happenings and events • Timely reactivity to changes that may have either a positive or negative impact • Ensure that different stakeholder needs, concerns or complaints are taking into account and duly addressed in accordance with organisational policy.	
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level) Basic Understanding of: Understanding of: Knowledge of: Advanced knowledge of:*	• Knowledge of external and internal communication and dissemination strategies • Knowledge of science and technology communication for non-expert target groups • Knowledge of target groups engagement strategies • Knowledge of design and identity branding • Knowledge of content creation and social media/traditional media management • Knowledge of behavioural change promotion towards cybersecurity actions • Knowledge of positive relationship building • Knowledge of programs and grants • Knowledge of governance and management practices • Knowledge of project management and budgeting • Knowledge of resource management • Knowledge of risk management • Knowledge of reputation management • Understanding of copyright and intellectual property rights issues, standards, and patent filing • Understanding of the multidiscipline aspect of cybersecurity • Understanding of the pressing social issues in the cybersecurity field • Social Responsibility	
e-Competences **(from e-CF)** *For quick access to e-CF Competences go to the e-CF Explorer:*	B.5. Documentation Production D.6. Digital Marketing	Level 3 Level 4

https://ecfusertool.itprofessionalism.org/explorer		

4.1.8 Management Leader

Profile Title	Management Leader
Alternative Title(s) *Lists titles under the same profile*	Coordinator Project Manager
Summary statement *Indicates the main purpose of the profile.*	The management leader is responsible for the operational management and technical vitality of the project encompassing management components on contractual, financial, legal, technical, administrative and ethical levels.
Mission *Describes the rationale of the profile.*	The establishment of a sound and flexible project management structure and an efficient management process as well as the provision of an effective risk management strategy, so as to avoid of deviations from the work plan.
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	Project quality plan, Project Handbook Risk Assessment Plan Innovation strategies
Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*	Project Management: • Organize, coordinate and lead the project team • Monitor and supervise the project progress • Monitor and control quality of the project/achievements • Observe and screen internal and external circumstances – react to unforeseen circumstances/developments • Ensure achievement of milestones and objectives • Ensure compliance with planned Budget Risk Management: • Ensures the proper handling and prediction of risks • Risk identification and risk analysis • Estimation of impacts and the definition of mitigation measures Innovation Management: • Efficiently monitor market needs and technical evolutions • Ensure that the project work plan is adjusted as needed in order to seek that the final results of the project are

Profile Title	Management Leader	
	implemented in such a way that they best meet the needs of the market	
Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	• Organization and monitoring • Team management – interpersonal skills and motivation • Effective Communication • Negotiation • Scheduling and Time Management • Leadership • Technical Expertise • Risk Management • Critical Thinking and Problem Solving	
e-Competences **(from e-CF)** *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	A4 Product / Service Planning E2 Project and Portfolio Management E3 Risk Management E4 Relationship Management E7 Business Change Management	Level 4 Level 3 Level 4 Level 5 Level 4

4.1.9 Program Leader

Profile Title	Program Leader
Alternative Title(s) *Lists titles under the same profile*	Cybersecurity R&I Programmes Portfolio Manager Cybersecurity R&I Programmes Director Cybersecurity R&I Programmes Officer Head of R&I Programmes
Summary statement *Indicates the main purpose of the profile.*	Manages and coordinates cybersecurity research and innovation strategy implementation and R&I programmes portfolio to ensure individual R&I programmes direction, cross-programme alignment, and synchronization, fit to strategic roadmap as well manages programmes intersection to achieve effective use of the resources, avoid duplication, synchronization of actions to maximize the success.
Mission *Describes the rationale of the profile.*	Defines, maintains, and communicates the cybersecurity R&I roadmap implementation vision, strategy, policies and procedures. Coordinates the implementation of the individual cybersecurity R&I programmes to fit strategic objectives. Coordinates individual R&I intersections. Coordinates research, innovation, academia, industry, SME, entrepreneurial, governmental and policy institutions' R&I activities to achieve consolidated impact. Assures timely information exchange across all stakeholders' groups.

Profile Title	Program Leader
Deliverable(s) *Illuminate the Profiles and explains relevance including the perspective from a non-Cybersecurity/ ICT point of view.*	• Cybersecurity Strategy implementation plan and report • Cybersecurity R&I Roadmap implementation plan and report • Cybersecurity R&I Programmes portfolio governance plan and report
Main task(s) *A list of typical tasks performed by the profile.* *is tasked to:*	• Adaptation, synchronization, progress measurement, and improvement for governance of R&D&I activities • Propagate cybersecurity strategy to individual Programs and Roadmap • Adapt strategic and high-level objectives to Programs and Roadmap • Defines, implements, and maintains governance framework. • Cybersecurity R&I Programmes portfolio governance and coordination: • Coordinating finance allocation and instruments design • Coordination of implementation efforts across activities • Consolidation of implementation results in the perspective of impact • Coordinated exploitation and operationalization • State-Of-The-Art management (library of states of SOTAs') • Coordination and support of uptake • Coordination of evolutionary aspects of all artefacts • Handle change management due to coopetition • Facilitate coopeting activities • Facilitate posterior use of results • Perform Programs comparisons • Measure progress with regards to Programs and Roadmap KPI • Review Programs and Roadmap risks • Improve objectives of Programs and Roadmap • Improve activities and processes of Programs and Roadmap from feedback loops • Ensure mutualisation of efforts • Ensure sharing of practices • Ensure transversal consistency between Programs, and with regards to Roadmap
Key skill(s) *A list of abilities to perform work functions and duties by the profile.* *Ability to:*	• Analyse and implement cybersecurity standards, frameworks, policies, regulations, legislations, certifications, and best practices • Communicate, coordinate, and cooperate with internal and external stakeholders • Apply relevant standards, best practices, and legal requirements for cybersecurity • Understand and apply different R&I management, governance

Profile Title	Program Leader	
	and organisational frameworks, processes, tools, and practices. • Establish a cybersecurity R&I governance plan • Understand and apply innovation development, maturation, productization, marketization, innovation uptake and operationalization models, processes, and governance frameworks. • Ability to lead multidisciplinary innovation development and management teams. • Develop, champion, and lead the execution of a cybersecurity R&I strategy • Influence R&I mission-oriented implementation culture • Understand core multi-organisational, cross-organizational, cross-border business processes • Ability to lead constructive conflict resolution to align and synchronize for strategic objectives implementation.	
Key knowledge *A list of essential knowledge required to perform work functions and duties by the profile.* *(Depending on the level)* *Basic Understanding of:* *Understanding of:* *Knowledge of:* *Advanced knowledge of:*	• Knowledge of cybersecurity frameworks, policies, regulations, legislations, certifications, and best practices • Knowledge of cybersecurity strategic objectives, goal, and roadmap • Knowledge of portfolio management • Knowledge of programs and grants • Knowledge of governance and management practices • Knowledge of project management and budgeting • Knowledge of research, development, and innovation (RDI) relevant to cybersecurity subject matters • Knowledge of resource management • Knowledge of risk management frameworks • Knowledge of conflict resolution practices • Knowledge of cybersecurity tactics, techniques, and procedures • Knowledge of cybersecurity methods, methodologies, tools, and techniques • Understanding of copyright and intellectual property rights issues, standards, and patent filing • Understanding of the multidiscipline aspect of cybersecurity • Knowledge of future cybersecurity threats, trends, needs and challenges in the organisation	
e-Competences	A.1. IS and Business Strategy Alignment	Level 4

Profile Title	Program Leader	
(from e-CF) *For quick access to e-CF Competences go to the e-CF Explorer: https://ecfusertool.itprofessionalism.org/explorer*	A.7. Technology Trend Monitoring	Level 4
	A.8. Sustainable Development	Level 4
	A.9. Innovating (not on products but on management)	Level 4
	B.2. Component Integration	Level 3
	C.4. Problem Management	Level 4
	D.8. Contract Management	Level 4
	D.11. Needs Identification	Level 3
	E.1. Forecast Development	Level 5
	E.2. Project and Portfolio Management	Level 5
	E.3. Risk Management	Level 4
	E.4. Relationship Management	Level 5

4.2 A methodology for a sustainable CCN

This section provides an update of section 1.3.2 of the DoA where the methodology that would then be deployed in SPARTA had been described. This methodology has since then evolved through the actual execution of the project and it has thus been rethought while taking into account the perspective of a sustainable CCN. As detailed in deliverable D1.1, the declination of the instruments from this methodology was revised as the execution of the pilot progressed: Partnership was elevated to the role of instrument while Governance was better categorized as an Enabler. The three instruments and the Enabler at the basis of this methodology are thus as follows:

- Instrument 1: Roadmap
- Instrument 2: Programs
- Instrument 3: Partnership
- Enabler: Governance & Management Activities

We refer to Figure 5 of the first SPARTA governance deliverable [Bootstrapping a CCN Pilot, PU, M12], for a view of how those instruments interrelate.

4.2.1 Instrument 1: Roadmap

In year 3, substantial progress was made in implementing governance aspects of the defined Roadmap and addressing evolutionary as well as maintenance aspects of the Roadmap. Through various SPARTA workshops, but also events and meetings with Associates as well as with other pilots and other communities updating roadmaps. This enabled SPARTA to validate evolutionary part of the roadmap and to refine it for the long-term perspective. There was close coordination with national research roadmap activities, so that topics from the SPARTA roadmap have already found their way into these national roadmaps. The roadmap is revised three times annually so that it reflects possible new threats and emerging new technologies, such as trustworthy open-source hardware.

Adherence to SPARTA's research governance activities evolution

The SPARTA roadmap was presented and discussed in internal and public SPARTA meetings as well as at several online workshops with external stakeholders. It was also presented in an internal ECSO meetings and inter-pilot meetings. In order to get feedback from a broader community,

questionnaires were put online asking for comments and contributions to sharpen the roadmap. During the last quarter of SPARTA implementation (March 2022), a final revision was conducted by roadmap committee to ensure that the delivered roadmap is up-to date by completion of the project.

Roadmap sustainability

The roadmap is regularly being revised and updated based on input from academia, industry and innovation community. Priorities proposed by other international initiatives (e.g., ECSO) have also been taken into account while it was made available for inter-pilot discussion and as a contribution to the overall future ECCC roadmapping activities. Additionally, the Roadmap instrument should also include and take into account unexpected events and evolve following them such as the rapid digitization of all communication methods due to the Covid19 pandemic on which the agility of the instrument played a crucial part.

Roadmap focusing mechanisms

Interactivity and feedback from a wide range of expertise proved to be the core mechanism to build a coherent and complete Roadmap. While the pandemic shuffled a bit the cards, this is achieved by organising synchronous meetings with interactive comment and discussion options (e.g., uni- & multilateral virtual meetings, workshops, etc.) as well as to open up an opportunity to make asynchronous contributions (e.g., online questionnaires). Through the structuration of these meetings and opportunity with different workflows, the inputs can be processed quickly in a structured manner to integrate in the Roadmap.

Thanks to the agile, iterative roadmap development in SPARTA, a roadmap release was able to be created annually allowing new findings to be incorporated into the new release within a very short time and dynamic changes to be taken into account promptly. Sustainable topics that are not subject to strong dynamics are also very important trends to include, such as an open-source strategy to increase digital sovereignty, in addition to the technology topics.

Cross pilot coordination

During SPARTA efforts to lead cross-pilot coordination efforts and harmonize the different pilot roadmaps the common mission of strengthening Europe's digital sovereignty, the importance of having multiple and different approaches combined was shown. These activities finally reached a consensus during the third year on how all four pilots can work together to achieve integrated ECCC roadmap and establish a consistent governance process.

Even though the SPARTA project has ended, governance bodies have showed high interest and will to continue the inter-pilot activities with other pilots still running their implementations. Ways to sustain these activities outside of the scope of the pilots with other actors producing roadmap of different approaches must be envisioned to recreate similar synergies.

4.2.2 Instrument 2: Programs

Technical programs can be taken as a construct where several individual innovative developments are organised and governed. Each of the programs in SPARTA is an example of such construction like the T-SHARK program, where more than 10 different solutions development was integrated as showed in Figure 4.

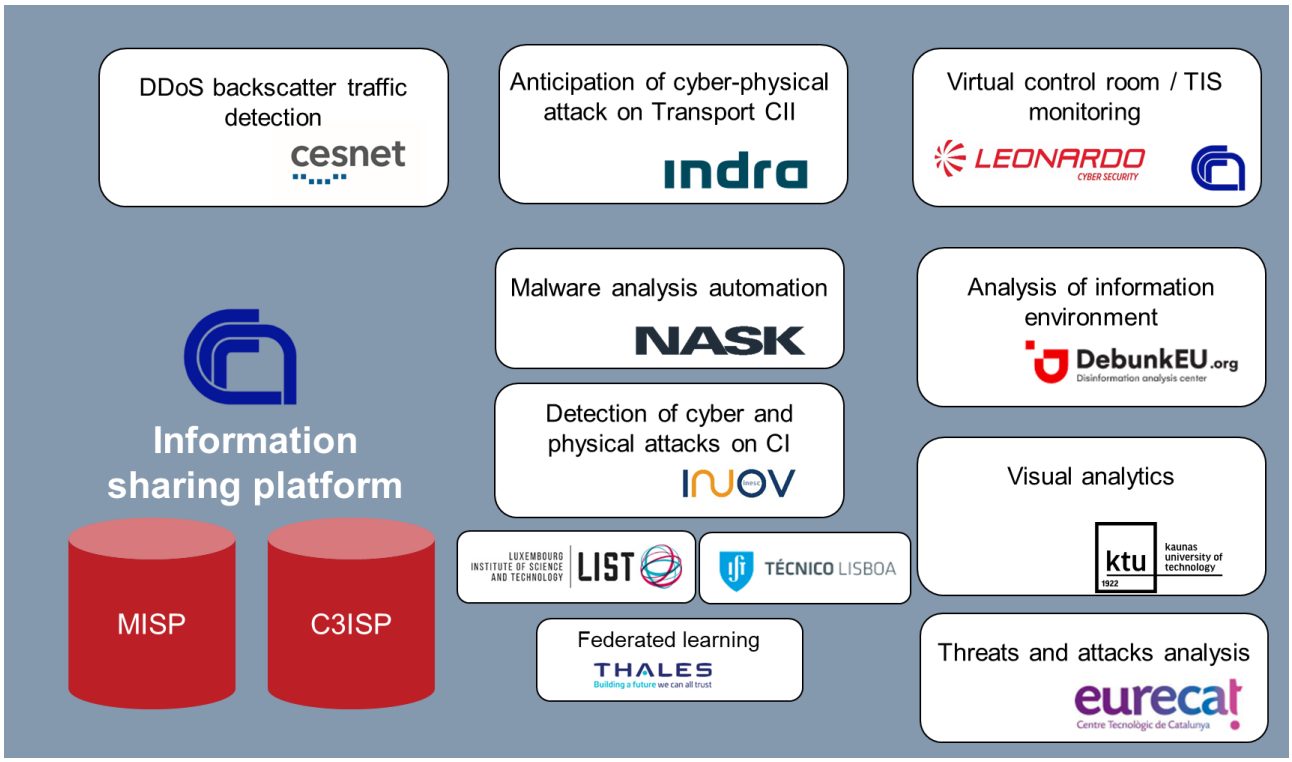

Figure 4: Illustration of Technical program scope.

Cross-fertilization

In such a model there is a need to have two level of cooperation mechanisms:

- Cross-programs
- Cross-integration within the program.

Further in this section we provide feedback on experiences of organising sustainable cooperation at both levels. We recognise the importance of financial aspect of sustainability cultivation. Project-based financing by design is not facilitating sustainability as organizations, including academia, RTO's, industry, tend to navigate from project to project. Common interest is another aspect, cultivating sustainability. This can be identified and exploited further using different cooperation and communication tools allowing to structure and guide commonalities. We additionally provide experience of organising sustainable cooperation in both levels, cross programs and within the program.

For cross-programs cooperation the concept of Visiting Committee (VC) was used. The aim of VC meetings was to find the possible synergies between the different programs, analyse the integration points and enrich research results. In addition, the role of this VC (described in D1.1) was also focused on facilitating internal and external SPARTA collaborative actions among performers.

During the project implementation, experiment-type VC meeting were organised between T-SHARK and all three other Technical programs. These produced tangible outcomes that are described in the respective reports with for instance a joint publication from one development in T-SHARK and SAFAIR program.

Well-structured and regular implementation of the VC concept can produce significant value for programs in terms of mission orientation, potential synergies (e.g.: similar data sets, useful outputs, etc.) and identification of new opportunities for further research and integration.

Organization of VC activities is not resource-demanding and can be part of overall governance activities. Such meetings should not be organised in the initial phase of programs activities. Fruitful VC meetings can be expected when programs are mature enough to see the full scope of their activities, are explainable and encounter limitations.

Another level of experimenting sustainable cooperation was done within the programs. Each program bringing their own collaborative approach which suited their need and objectives. For instance, during the initial stage of the T-SHARK development, it was observed that all individual innovative developments were very technology centric, measured mainly through TRL. It made them difficult to describe in a way understandable for others, including end-users, internal and external stakeholders.

Those observations led to the search for instruments to common governance of innovations. For this, focus was made on structuring process of end-user involvement, application of frameworks, enabling to describe individual developments, facilitation of cross-integration and identification of up-take fit issues. This led to the addition of other indicators into the T-SHARK process such as Maturity or System readiness level.

Common goal

A common integration end-goal proved to be an important aspect of the different programs, whether it is the Umbrella case of T-SHARK, the two verticals of CAPE, the unified use case of HAII-T or the AI competition in SAFAIR. It allowed to place all technological developments together in one view map, illustrating the multi-vectorial scenarios developed in each Program. It is interesting to note the coopetition difference between the programs, with the fully cooperative CAPE and HAII-T, the competitive SAFAIR and the hybrid T-SHARK. Each of them proved their benefits and allowed a program made of expert to produce concrete and fruitful results. A more complete presentation of the different programs can be found in their respective deliverables and in the above section.

Overall, the common integration goal for each program allowed to see how technical solutions are triggered and what outputs they can share with other (basic data and additional insights / information that can be valuable). It also allowed to place all developments in a common view, demonstrating how they are linked and how value from individual developments is cumulated. Figure 5 shows an illustration of this mapping for the T-SHARK program.

It is relevant to note, that selection and application of instruments is very situational. Timely recognition that certain instruments are not providing expected value, experimenting with new instruments is an important aspect. Thus, appropriate resources and flexibility are main factors of sustainability cultivation in project based activities.

Sustainability insights

Besides the experimental application of different instruments to facilitate sustainable cooperation, there are some other observations that are relevant to sustainability:

- Even though R&I&D projects need to be supported by ELSA, this has to be done gradually, as at the initial stage this will not be a support, but overhead. Programs or projects are not aware about all relevant details or limitations they face at the starting stages though they will benefit from by-design approaches;
- As environment changes very rapidly, there is a need for a more flexible execution model. They can be combined with Agile Stage Gates (ASG), shifting deliverables, extended financing, etc.
- In many cases, value created within the project is not exploited further, so post-project governance is subject to be considered.

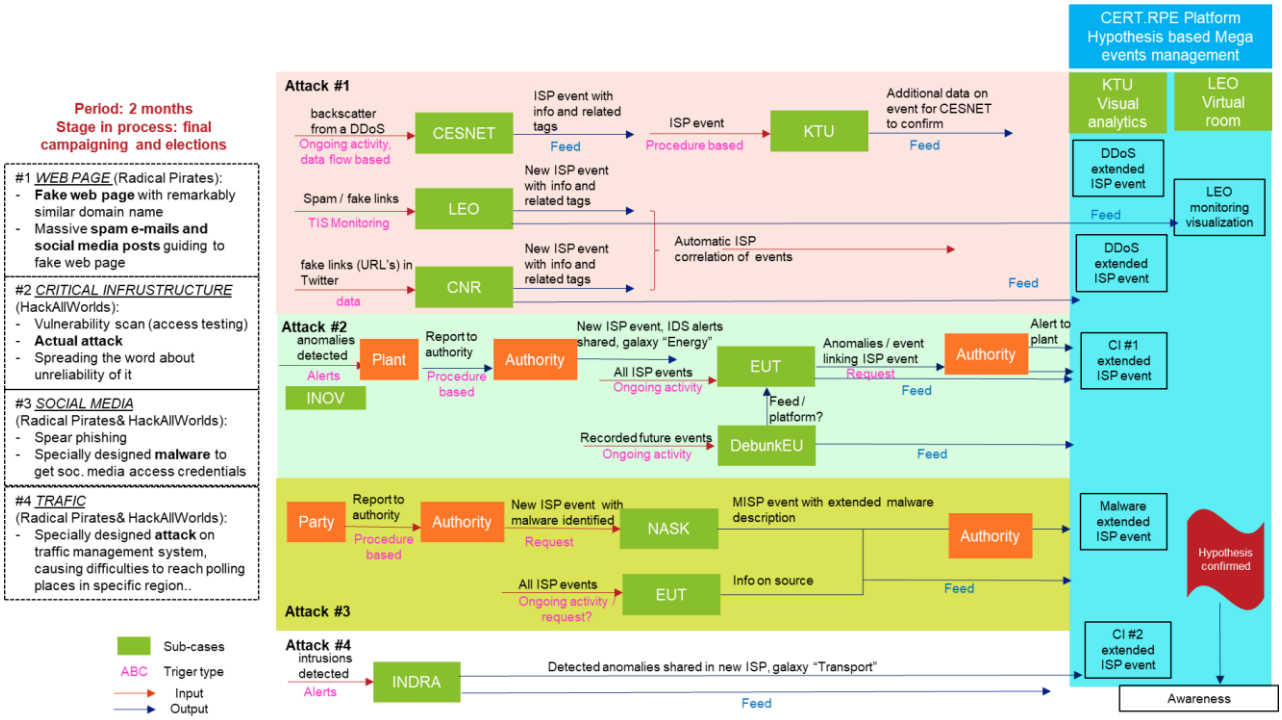

Figure 5: Illustration of Umbrella case application.

4.2.3 Instrument 3: Partnership

The Partnership Committee, led by the Partnership Director, contributed to the design and maintenance of the network's partnerships, including the Associates Council. It sets up space, time, and means to enable research collaborations, leveraging the strengths of existing structures and organizations of the SPARTA partners. As part of it, the committee, with other SPARTA bodies, contributed to the selection of the SPARTA membership, the organization of the SPARTA monthly workshops – that have been held in all the countries of a SPARTA partner, and those have been supported by the SPARTA ecosystem.

The pandemic forced us to run many of these events in virtual format. The Partnership Committee also created and updated the map of platforms and infrastructures – pivotal in focusing data, software and expertise resources – and developed the JCCI platform. It also promoted the cooperation among the SPARTA partner/associates/friends for new project/research activities and initiatives through the series of SPARTA brokerage events that triggered several cooperation. Overall, it promotes the cooperation among SPARTA ecosystem and with the other Pilots in serving the interests of European research and innovation teams. The partnership program has been set up in several layers of commitment and trust (associates and friends), in order to be flexible enough to accommodate the diversity of the stakeholders in Europe.

Overall, it is worth to mention that associates/friends were looking for "resources" to collaborate with SPARTA partners and the additional idea of SPARTA brokerage events in order to ease joint project proposal was welcome. Any instrument for partnership should consider substantial incentives for cooperation.

4.2.4 Enabler: Governance & Management activities

As an enabler, SPARTA's governance ties the previous 3 instruments together and supports the network research and innovation activities. In addition to the bodies mentioned in the previous instruments, SPARTA's governance is built around key activities with powerful leadership and diversity:

- Strategic Direction

The Strategic Direction coordinated the governance; in particular, it supervised the execution of the network's strategy and assigned tasks to meet high-level analysis requests. It conducted information sharing of key developments in the spheres of scientific policy-making, community-building initiatives, international events, and, to a lesser extent, geopolitics. The Strategic Direction has been solicited for strategic decision-making in the SPARTA project.

- Training and Awareness Taskforce

The Training and Awareness Taskforce provided its expertise on current development in the area of cybersecurity education, training and awareness. It has collaborated with national bodies, such as NCCCs, and European bodies, such as CCN and ECCC, to provide widely-accepted and high-impact results, in particular useful for creation of novel cybersecurity curricula and tools for their support. The team also stresses the practical impacts of the deliverables, supporting practical, usable results in the form of software and infrastructures. The sustainability of results playing a critical role, partners such as ENISA and CCN have been present in most of WP9 activities. Latest development and lessons-learnt from WP9 are transferred into all-SPARTA activities, such as Roadmapping, Governance or Networking.

- Certification Taskforce

The Certification Taskforce, under the direction of the Certification Officer, provided expert inputs on the state-of-the-art, gaps, and advances in the field of cybersecurity certification. It has provided insights on the process and tools required in building next-generation certification tools, and helps identify potential areas of the Roadmap and Programs that can be of interest in building these capacities – either directly through progress in evaluation and conformity, or indirectly through advances in the development of specific security functions. A certification task force should focus on supporting with methods, processes and tools for the future Cyber Act certification schemes. As was explained in D1.3 and WP11 deliverables, the process of creating new Cyber Act certification schemes, evaluating, and updating them is the responsibility of the Commission and ENISA. The work of the Certification task force should be seen as complementary to this work, by supporting the certification schemes with recommendations on methods and tools for both the certification evidence gathering phase and the certification evaluation phase.

- Dissemination Committee

The Dissemination Committee, under the direction of the Dissemination Officer, provided communication expertise and tools for the network. It has ensured these tools are available across project boundaries, that communication exploits state-of-the-art (in particular digital) mediums while taking place in full respect of the constraints of the field and its practitioners. The Dissemination Committee ensures coherent and regular internal communication between actors and public communication to the European community. It strives for cross-collaborations with other European actors in the cybersecurity and digital sector, such as CCN and ECCC, to achieve a higher reach and visibility. The Committee works towards closing the cybersecurity gender and diversity gap through actions ranging between research, targeted events and workshops.

- Ethics Committee

The Ethics Committee, under the direction of the Ethics Officer, addressed proactively the major ethical, legal and societal aspects relevant in the context of large-scale cybersecurity research and innovation in transnational competence networks. It has paid particular attention to specific issue topics arising in technical activities but has also investigated questions of general interest to the entire cybersecurity research and innovation community. It set up and maintained appropriate procedures, criteria, templates, information sheets, potential opinions and approvals from relevant entities, explanations, and relevant compliance documentation as well as descriptions of technical and organizational risk-mitigation strategies and measures (including security ones) implemented to comply to the ethics requirements. It is important that the Ethics Committee can act independently and address any issue of which it becomes aware. From a governance perspective, the members composing this body were also active partners in SPARTA such that each Programs has one Ethics Committee member involved at this heart. This is designed to help spreading ELSA good practices, detect potential issues, and handle them from solution design to implementation.

Chapter 5 Summary and Conclusion

Throughout this document, SPARTA delivers a thorough synthesis and outlook for the governance aspects for Programs and Activities, anchored in concrete skills and instruments requirements, with the goal to sustain the modular governance of a high risk – high reward cybersecurity competence network.

Quite remarkably, these recommendations are the result not only of internal design and exercises, but they have the advantage of having being applied concretely, and extensively, at all levels of SPARTA's execution. Even further, it has held true to its goal of leading the way in growing reflective, self-aware governance mechanisms, with a demonstrated capacity to elicit and integrate external and internal recommendations on a regular basis.

In this regard, we can clearly state that SPARTA has completed its mission to "propose, test, validate and exploit the possible organisational, functional, procedural, technological and operational setup of a cybersecurity competence network". It has shown, as a result, how this concrete governance model can give rise to world-leading, mission-oriented research and innovation actions in Europe.

Chapter 6 List of Abbreviations

Abbreviation	Translation
AI	Artificial intelligence
AG	Arbitrage Group
APER	Assessment of Pre-Existing Resources
ASG	Agile Stage Gates
CAB	Conformity Assessment Bodies
CCC	Cybersecurity Competence Centre
CCN	Cybersecurity Competence Network
CERT	Computer Emergency Response Team
C3ISP	Collaborative and Confidential Information Sharing and Analysis for Cyber Protection
CSIRT	Computer Security Incident Response Team
DoA	Description of Actions (Project Plan)
DMP	Data Management Plan
EB	Executive Board
EC	European Commission
ECCC	European Cybersecurity Competence Centre
ECCN	European Cybersecurity Competence Network
ELSA	Ethical, Legal, Social Aspects
ENISA	European Network and Information Security Agency
ETACS	Electronic Time Attendance Control System
EU	European Union
IDPR	Identification and Documentation of Produced Results
IT	Information Technology
JIP	Joint Initiatives Program
KPI	Key Performance Indicator
MISP	Malware Information Sharing Platform
MRL	Manufacturing Readiness Level
NCCC	National Cybersecurity Competence Centre
OSS	Open Source Software
RAMP	Research Assets Management Platform
RDI	Research, Development and Innovation
RFG	Roadmapping Focus Group
SD	Strategic Direction
SDL	Service Description Language

SG	Stage Gates
SotA	State of the Art
SRL	System Readiness Level
SSH	Social Science & Humanities
VC	Visiting Committee
WP	Work Package

Chapter 7 Appendix – SPARTA Satisfaction Survey

*Welcome to the survey for members and associates/friends of the SPARTA consortium. This **short survey** will take no more than **5 minutes** of your time.*

This survey is part of the assessment of the SPARTA governance, a study that is conducted by Technopolis Group, an independent consultancy agency. The study is commissioned by CEA Tech.

*We would be very grateful if you could answer this survey before **Friday, March 26**. All your answers will be treated confidentially. We respect your privacy and protect your personal data according to GDPR. For further information see Technopolis Group's Privacy Notice.*

1. **Please indicate which of the following best describes the organisation you're affiliated to? (select one)**
i) Higher Education Institute
ii) Research Organisation
iii) Large/Medium Enterprise
iv) Small and Medium Enterprise (SME)
v) Public administration body
vi) Other (please specify): open text box

2. **Is your organisation a member of the SPARTA consortium? *Choose one***
i) Yes, my organisation is a member of the consortium
ii) No, my organisation is an Associate/Friend of SPARTA

ROUTING:

- **if i) go to Q3**
- **If ii), go to Q4**

3. **To what extent do you agree with the following statements?**
Not at all, To a limited extent, To a moderate extent, To a large extent, To a very large extent, Don't know
i) The **SPARTA roadmap and its Y2 update** responds to the current policy needs and priorities in the field of cybersecurity
ii) There are a sufficient number of **opportunities for consortium members** to discuss and provide input to SPARTA's technical and non-technical activities

i) There are a sufficient number of **opportunities for associates/friends** to discuss and provide input to SPARTA's technical and non-technical activities
ii) The online SPARTA **challenge/feedback form** is a useful tool to flag new challenges for the SPARTA roadmap to include
i) The inclusion of a WP focused on **ethical, legal and societal aspects** (ELSA) ensures the ongoing alignment of SPARTA with policy needs and priorities

4. **To what extent do you agree with the following statements?**
Not at all, To a limited extent, To a moderate extent, To a large extent, To a very large extent, Don't know
i) The **SPARTA roadmap and its Y2 update** responds to the current policy needs and priorities in the field of cybersecurity
ii) There are a sufficient number of **opportunities for associates/friends** to discuss and provide input to SPARTA's technical and non-technical activities
iii) The online SPARTA **challenge/feedback form** is a useful tool to flag new challenges for the SPARTA roadmap to include

ROUTING:

- **if i) go to Q5**
- **If ii), go to Q9**

5. **In which WP are you mainly involved?** ***Choose one***
Scroll-down menu – WP1 till WP13 / with titles

6. **Is your organisation leading a WP?** ***Choose one***
i) Yes
ii) No

7. **Compared to your initial expectations, how well has SPARTA succeeded in reaching the following objectives?**
Much less than expected, Less than expected, As expected, More than expected, Much more than expected, Don't know
i) The investigation of new ideas aimed at fostering transitions
ii) The integration of the most relevant emerging scientific challenges into the SPARTA roadmap

iii) The geographic and disciplinary diversity of the SPARTA members
iv) The geographic and disciplinary diversity of the SPARTA Associates and Friends
v) The creation of a community around SPARTA that allows for gaining insights on new scientific/educational challenges
vi) An optimal coordination and knowledge exchange across activities, work packages and governance bodies/teams thanks to the matrix structure
vii) Communication among partners, ensuring all participants are up to date with the main activities and outcomes of SPARTA
viii) The visibility of SPARTA's activities and achievements to the target audiences and 'external' environment
ix) The adoption of Responsible Research and Innovation and attention for ethical, legal and societal aspects (ELSA) throughout all activities and practices in SPARTA

8.	**To what extent do you agree with the following statements?**
	Not at all, To a limited extent, To a moderate extent, To a large extent, To a very large extent, Don't know
i)	The **SPARTA meetings** are a useful platform for members to discuss and provide input for the review of the SPARTA roadmap
ii)	SPARTA is sufficiently open to non-member industry actors enabling knowledge exchange
iii)	There is an appropriate level of attention for interaction with other cybersecurity initiatives in SPARTA
iv)	There is an appropriate level of attention for **interaction with the other pilot projects** creating synergies and coherence
v)	There are a sufficient number of **interactions with other projects and initiatives** to be able to capture and integrate new scientific/educational challenges
vi)	There is a sufficient **level of international collaboration** to be able to capture and integrate new scientific/educational challenges
vii)	The **Committee meetings** are key to ensuring the appropriate knowledge exchange between SPARTA activities and WPs
viii)	The **Strategic Direction meetings** are key to ensuring the exchange of knowledge across WPs and activities
ix)	The **Strategic Direction meetings** are key to ensuring action is taken upon new scientific/educational challenges
x)	The number of meetings is appropriate when considering the project governance and management needs
xi)	The time invested in meetings weighs up to the meetings' value in terms of internal knowledge exchange
xii)	The internal reporting requirements are necessary and well-organised

xiii) The internal reporting requirements are shared among the SPARTA partners in an appropriate manner

9. **To what extent do you agree with the following statements?**
Not at all, To a limited extent, To a moderate extent, To a large extent, To a very large extent, Don't know
i) The **Associates Council and Associates Workshops** are important platforms to gain or provide insights on new scientific/educational challenges
ii) SPARTA shows an appropriate level of **openness** towards non-members in terms of access to tools and information
iii) SPARTA shows an appropriate level of **inclusiveness** towards non-members in terms of their areas of activities (industry, public agencies, non-technical organisations etc)
iv) **Access to the resources** in the Joint Competence Centre Infrastructure is of high importance and value for my organisation

10. Is there **any other aspect related to the SPARTA governance practice** that you would like to share with us?

[*open text box*]

Thank you for your time. Your response has been saved. You can close this window now.

Chapter 8 Bibliography

1. te Kulve, H., Rip, A.: Constructing productive engagement: pre-engagement tools for emerging technologies. Science and Engineering Ethics 17, 699-714 (2011)

2. Schuurbiers, D., Fisher, E.: Lab-scale intervention. EMO reports 10, 424-427 (2009)

3. Hagendorff, T.: A Virtue-Based Framework to Support Putting AI Ethics into Practice. Philosophy & Technology 35, (2022)

4 ENISA European Cybersecurity Skills Framework (draft), April 5, 2022.

5 IEEE Standard Model Process for Addressing Ethical Concerns during System Design. Systems and Software Engineering Standards Committee, New York, 2021.