D1.6

From assessing to supporting the future 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 / D1.6 / V1.0
Work package contributing to the deliverable	WP1
Due date	July 2022 – M41
Actual submission date	21st September 2022

Responsible organisation	Fraunhofer
Editor	Dirk Kuhlmann
Dissemination level	PU
Revision	V1.0

Abstract	This document assesses the structures, processes and activities related to the governance of the SPARTA pilot during its final phase. The approach is qualitative and pragmatic in analysing these activities in regard to their continued relevance for the ECCC and the ECCN. The current and future degree of the implementation of these institutions is taken into account, as well as novel challenges arising from contextual changes during the pilot's lifetime. Methods and results from previous assessments are analysed in view of their continued applicability in real-world scenarios.
Keywords	Governance, pilot, structure, process, Cybersecurity Competence Network, Cybersecurity Competence Centre, CCN, ECCC, NCC, assessment, external

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

Editor

Dirk Kuhlmann (Fraunhofer)

Contributors (ordered according to beneficiary numbers)

Michael Friedewald (Fraunhofer)

Reviewers (ordered according to beneficiary numbers)

Ana Ayerbe Fernandez-Cuesta (TEC)

Bertrand Lathoud (SMILE)

Disclaimer

Table of Content

List of Tables

Chapter 1 Introduction

This report is the last of three studies on governance aspects of SPARTA, an EC funded project for piloting the European Cybersecurity Competence Centre (ECCC) and Network (ECCN). It describes the pilot's investigations and research in support of governing the ECCC, the ECCN, and its national counterparts, the National Coordination Centres (NCCs) in 27 member states.

The first study addressing these issues (D1.2, end of 2020) used a pilot-internal perspective, addressing both management and governance aspects of the pilot during the first work period. The DoA of SPARTA foresaw a lightweight process, and standard assessment methodologies such as COBIT turned out to be too heavyweight for this purpose. The D1.2 assessment therefore relied on tailored methods. These were chosen with industry-grade methodologies in mind to allow future comparability of results if so required. The applicability of COBIT assessment methods was demonstrated in WP2 by way of case studies on auditing and supervising activities regarding ethical, legal and social (ELSA) aspects. This is documented in SPARTA's deliverables D2.2, D2.4 and D2.7.

The following study on pilot governance (D1.4, mid 2021) covered SPARTA's second work period and assumed an external perspective. It included an independent assessment of an independent evaluation entity. The external assessment analysed SPARTA' governance with regard to its key performance indicators (KPIs) which reflect the requirements spelled out in the original Call for Proposals (CfP) for the pilots. It was complemented by an analysis from consortium member Fraunhofer ISI. The corresponding part of the study concerned the applicability of SPARTA's findings about pilot governance objectives, structures and mechanisms to the real-world implementation ECCC and ECCN. Its results are preliminary, since the analysis only reflected the progress towards the practical implementation of the ECCN that had been made from early 2020 until mid-2021. Up to that point, Regulation (EU) 2021/887[1] had been finalized, the decision on Bucharest as location for the ECCC headquarter had been taken,[2] the kick-off of ECCC board meetings[3] had taken place, and EC had made initial contacts with the newly appointed NCC representatives[4].

The project duration originally anticipated in SPARTA's DoA was 36 months, running from February 2019 to February 2022). This duration was extended by 5 months in January 2022, enabling the project to monitor the first phase of implementing the ECCC and the NCCs. At the time of writing this report, SPARTA is in the process of being wrapped up.

The purpose of this study is to take stock of SPARTA's work on governance in face of the progress made towards practical implementation of the ECCC, the ECCN and the NCCs. These real-world activities serve as analytical background to evaluate a range of options and activities originally (2018) envisaged for investigating governance aspects of the ECCC. These options are spelled out in detail in the Call for Proposals for CCN pilots and SPARTA's DoA. In the context of this study, they will be contrasted with the practical realities created by directive (EU) 2021/87 and the implementation activities that have since then been carried out.

---

[1] Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.
URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32021R0887

[2] Laurens Cerulus: 5 reasons why Bucharest won the EU cyber center race. Politico Pro, 11. December 2020
URL: https://www.politico.eu/article/5-reasons-why-bucharest-won-the-eu-cyber-competence-center-race/

[3] European Commission: The European Cybersecurity Competence Centre and Network moves forward: future Governing Board meets for the first time. Press release, 16 April 2021.
URL: https://digital-strategy.ec.europa.eu/en/news/european-cybersecurity-competence-centre-and-network-moves-forward-future-governing-board-meets

[4] European Commission: Workshop of National Coordination Centres. Event publication, 25 May 2021
URL: https://digital-strategy.ec.europa.eu/en/events/workshop-national-coordination-centres

The final form of (EU) 2021/887 presented a number of issues not anticipated by the EC's 2019 CfP for ECCC pilot projects. Notably, this concerns details of the future interactions between the European Competence Centre and the National Coordination Centres and structure and the dynamics of the ECCC governance boards. Both at executive and strategic level, the operation of these boards will be influenced by national preferences and voting arithmetic linked to the level of financial contribution of member states.

The study shows that SPARTA abandoned several lines of investigations on governance for good reasons. In almost all of these cases, the DoA had assumed a level of trans-EU consensus, shared jurisdiction, or commonalities of competence and responsibility that did not match the outcomes of political negotiations for (EU) 2021/887 and the realities found in practice. While SPARTA's governance structure turned out to be remarkably similar to the one adopted for the ECCC, many aspects of pilot governance processes, including its success criteria, are not directly applicable to the real-world scenario. Results from D1.2 and D1.4 will have to be revisited in view of their continued relevance.

There is a distinct possibility that NCCs will be competing amongst each other for EC funding in future. This scenario could not be modelled with the lean governance structures of an ECCC pilot or as an inter-pilot activity. Central ECCN aspects, such as the NCC service catalogue or the rules and considerations governing the balance of cybersecurity RD&I funding at European and national level, are still under development. This exemplifies that important questions regarding ECCN governance could not be addressed by the ECCN pilots. To give some further examples:

- The barrier for applying for EC research funding has traditionally been high. Can the processes for defining research programs, creating proposals and performing reviews be simplified for projects funded through FSTP mechanisms? Is it possible lower the bar for SMEs and Start-Ups, e.g. by reducing the amount of front-loaded effort, the burden of management and reporting, and by loosening admission criteria regarding their financial standing and business continuity?
- How can we determine the relevance of small-scale financial incentives such as the envisaged FSTP research grants for galvanizing cybersecurity RD&I? (Note CCN pilots had no resources to carry out practical experiments of this kind with members of their respective "satellite systems" of partners and friends.)
- Are there opportunities for joint research with technology partners from natural political allies such as Japan, South Korea, Taiwan, Singapore, or Israel?
- With the UK leaving the EU, the link to cybersecurity activities pursued by the '5-eyes' states (United States, United Kingdom, Australia, New Zealand, and Canada) has been severed. What are the options and guiding principles for re-vitalizing research cooperation with these countries?
- Will the policy of NCCs managed FSTP projects continue favour openly accessible publication, and how will this be balanced against prerogatives of national secrecy?
- What are the implications of NCCs mediating the access to a "national cybersecurity community"? What claims of authority sets such a group apart from self-selected cybersecurity communities from academia, industry and civil society?

These are just some of the factors that will influence the future operations ECCC and NCC, but are beyond the scope of what could be investigated by SPARTA and the other pilots, and regarding these questions, no evidence-based advice or support can be provided.

In contrast to the methodology driven studies D1.2 and D1.4, the vantage point of this study has been selected pragmatically; activities related to SPARTA's work on governance are presented in view of their continued relevance and their practical applicability for the ongoing implementation of the ECCN.

The evolution of the ECCC and ECCN implementation is accounted for up to mid-summer 2022; cutting off with the last batch of decisions by Governing Board that date from July 23 2022. We present a brief historic timeline, a snapshot of new challenges,

Chapter 2 Dimensions and Constraints of Support

Five years after Jean-Claude Juncker's initial announcement[5], the practical implementation of the European Cybersecurity Competence Network is well underway and the contours of the ECCC and the NCCs are becoming visible. To clearly understand the dimensions and constraints of this institutional nexus, and the type and level of support that can be offered by SPARTA's governance activities, it is useful to briefly recapitulate the history that led up to this point.

2.1 Context, Purpose and Objectives of the ECCC and the ECCN

The institutional constellation of an ECCN consisting of an ECCC and NCCs originates from an EC initiative from 2017. By then, the impact of cybersecurity attacks and ransomware had reached a point that called for decisive actions at the governance level. In this situation, the EC formulated a strategy to coordinate cybersecurity related activities of EU member states with policies European level, with the stated objective of better dealing with and defending Europe against cyber-attacks[6]. A core element of this program was the creation of a cybersecurity competence centre at EU level helping to strengthen cybersecurity at across the EU by supporting RD&I on products and services[7].

This aim is complicated by the fact that the EU and its institutions have no mandate to interfere in policy areas of national security or defence. Traditionally, cybersecurity has been regarded as a matter of national security and is closely guarded by national prerogatives and pre-legislation. It was clear from the outset that no trans-EU agreement could be expected to delegate these powers and that the EC had to operate within the limits of its existing mandate.

Establishing a cybersecurity centre with powers of coordination at European level therefore required endorsement and stakeholdership of all EU member states, and to set up this centre, the EC had to employ instruments that were within its mandate. In the past, four EU policies had perceptible effects on driving IT-security related initiatives, namely (1) the protection of civil and consumer rights, (b) the establishment of a common market, (3) the protection of European networks and infrastructures, and (4) research policy. Out of these options, the strategic provision of research grants was chosen as the most suitable one for driving the creation of a new institution.

By 2019, an updated outline for a European Cybersecurity Competence Centre was presented which envisaged no actual operative cyber-intelligence or defence capacities. The corresponding announcement[8] re-iterates the plan for an ECCC, but does not mention any specific objectives that would have required endorsement of individual member states. Instead, the official mission statement was confined to the main objective of "sharing threat intelligence and cybersecurity knowledge through setting up dedicated centres with reporting duties to national authorities in case of serious incidents"[9].

Negotiations between the member states and the EC established some additional cornerstones. Regarding the institutional setup and the core tasks, the political compromise envisaged an ECCC operating as the nub of a network of national cybersecurity centres. These NCCs would contribute to a coordinated research agenda and organize cybersecurity communities at national levels. In return, the NCCs would receive research grants from the EC that could be used in pursuance of national cybersecurity initiatives. Supplemented by contributions at national level, these grants

[5] European Commission: President Jean-Claude Juncker's State of the Union Address. Sep 13, 2017 URL: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_17_3165
[6] see previous footnote
[7] European Commission: State of the Union -- Cybersecurity: Commission scales up EU's response to cyber-attacks. Sep 19, 2017.URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3193
[8] European Commission: Speech by President-elect von der Leyen in the European Parliament Plenary on the occasion of the presentation of her College or Commissioners and their programme. Nov 27, 2019. URL: https://ec.europa.eu/commission/presscorner/detail/en/speech_19_6408
[9] see previous footnote

handed out as cascaded funds for RD&I. at a national level. This is a marked change from the traditional EU funding for cybersecurity research, as the new setup allows dedicated national research programs to be co-funded using EU resources. Over time, interactions between ECCC and NCCs could help to align national and EU cybersecurity strategies and programs.

Other desirable results of this initiative would be better adoption of results from cybersecurity research by the market and the alleviation of the fragmented European cybersecurity market[10], which is characterized by an absence of global players, scattered resources and underinvestment. These deficits have been recognized for a long time, and in 2016, the ECSO cPPP was created as an industry- driven initiative in an attempt of mobilizing additional capital.

However, investment in cybersecurity RD&I has continued to lag behind when compared internationally. This puts into question whether industry and market-driven strategies alone can suffice to safeguard European competitiveness. The constant growth of budgets for cybersecurity research in the context of H2020, HORIZON EUROPE and DIGITAL EUROPE and the implementation of the ECCC can be taken as indicators that more support from governmental sources is deemed necessary for helping to maintain cybersecurity in Europe and to change the market conditions accordingly.

Obviously, a real-world impact of this magnitude and scale cannot not be expected from the ECCC pilots, which are working within their constraints of fixed duration and budgets and research agendas pre-established by their proposals and DoAs. Future will tell whether significant shifts in terms of strategic direction or market can be triggered by activities of the real world ECCN, once its institutions have reached full financial autonomy and operational capability. For the time being, the ECCC will gradually take over tasks that are currently executed by the EC on its behalf, oversee the first round of FSTP funding administered by the NCCs, and drive a co-ordinated research agenda for the final calls of DIGITAL EUROPE and subsequent EC programs. Given the increasing relevance of cybersecurity, the ECCC should broaden its influence towards all DGs and program elements concerned with defining and implementing the European strategy for digitalization.

In this context, it should be noted that demands for improved cybersecurity capabilities also come from the security and defence sector, but related research is typically not funded in the context of civilian programs. Synergies can be achieved, though, by research on dual-use technology. EU Member States may also align their cyber defence activities with the Framework of Permanent Structured Cooperation (PESCO) and the European Defence Fund[11], and given the background of an ongoing war at the eastern border of the EU, these calls carry even greater weight today.

Notwithstanding existing constraints of influencing cybersecurity at the European level, the strategic, financial and administrational support of the ECCC can substantially contribute to improving international coordination, creating and mobilizing human and technical resources, and to fostering a cybersecurity ecosystem at European scale. The permanent institutional setup of ECCC and NCCs will operate on an annual budget of an estimated €40M[12]. The institutions will be responsible for distributing hundreds of millions worth of R&D grants during the HORIZON EUROPE and DIGITAL programs. Their task is to improve the preparedness, awareness, reactivity and reduces Europe's exposure to cyber-threats[13], and they will have account for the impact of their work towards these goals. So far, however, the requirement of perceptible impact for European citizens, organizations and public bodies is not reflected by the indirect KPIs for the ECCC and ECCN as defined in directive 2021/887. These KPIs may need to be extended.

[10] European Commission: Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap. Oct 27, 2017
URL: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/su-ict-03-2018
[11] see previous footnote.
[12] Estimate, assuming 1-2ME annual operating costs for each NCC
[13] European Commission: Cybersecurity in Horizon Europe & Digital Europe. URL (last retrieved 2306.2022): https://cyberwatching.eu/sites/default/files/Cybersecurity%20in%20Horizon%20Europe%20Digital%20Europe_20210713.pdf

This brief historic account should serve as a reminder that the explicit goal of the initiative leading up to the implementation of the ECCC (and the corresponding CfP for piloting activities) was to improve the state of cybersecurity in Europe in practice, that is, "on the ground". The tasks of the ECCN are predominantly of strategic and coordinative nature, so measuring the direct impact of its contribution towards practical goal may turn out to be challenging. Still, the factual improvement of Europe's cybersecurity capabilities and capacities will be the measuring bar for gauging the effectiveness of the new institutional constellation. Time has moved on since the ECCC were conceived, and during their lifetime, a number of new challenges have come to the fore that will influence the future direction and operation of the ECCN.

2.2 Current Challenges

To play its anticipated role of orchestrating cybersecurity security research at European and national level, future ECCC activities will have to account for a number of challenges that have become pronounced during the final phase of the pilots:

1. **Mobilization of National Cybersecurity Communities:** One objective of SPARTA was to establish a governance structure for an ECCN that supported its research-oriented stance as well as the coordination of a competence network capable of addressing today's cybersecurity problems. This effectively resulted in a two-tier structure. The first tier consisted of consortium members directly involved in the pilot. The second tier was the community friends and associates who followed the SPARTA's progress, thereby obtaining information and guidance about the evolution of the European cybersecurity landscape and agenda. The role and structure of both groups exemplifies a preliminary instantiation of a future cybersecurity competence community foreseen by directive 2021/887 (note that this regulation does not include details about these community, apart from their members being organizations located within the realm of the ECCC).[14]
   The admission policy of SPARTA's "friends and associates" accepted members from all EU member states and was based on self-selection. In contrast, ECCN community membership is organized along national lines, and it involves an admission process. The first challenge will be to direct and channel pilot consortium members and associates towards participating in national competence communities. The provision of regulation (EC) 2011/877 may limit the participation of informal, civic communities and individual experts. The NCCs should therefore consider organizational measures for facilitating the inclusion of loosely knit civic and local communities, "cyber regions" and skilled individuals.

2. **Operational capabilities of the ECCN in the short to mid-term future:** The Cybersecurity and Trust part of the Digital Europe 2021-2022 programme has an indicative budget of € 269M allocated to one Specific Objective 3 "Cybersecurity and Trust". Nominally, all topics are overseen by the European Cybersecurity Industrial, Technology and Research Competence Centre with the Network of National Coordination Centres. However, this part of the programme will effectively be implemented by the Commission on behalf of the ECCC and NCCs,[15] since these institutions do not yet have the capacities for managing sub-programmes at scale.
   The low response to the first call offering financial support for the deployment of NCCs (CYBER-02-NAT-COORDINATION) is indicative for the current provisional state of the ECCN. The EC has set aside € 66M to support each of the 27 NCCs with up to € 1M for

[14] Decision 2022_08 of the ECCC Governing Board endorsed a number of more specific rules. While these are only guidelines, they are likely to be adopted by the NCC's, given that they were jointly created and endorsed by the ECCN.
[15] European Commission: Annex to the Commission Implementing Decision on the financing of the Digital Europe Programme and adoption of the multiannual work programme - Cybersecurity for 2021 - 2022. C(2021) 7913 final, 10.11.2021. URL: https://ec.europa.eu/newsroom/repository/document/2021-46/C_2021_7914_1_EN_annexe_acte_autonome_cp_part1_v3_x3qnsqH6g4B4JabSGBy9UatCRc8_81099.pdf

operational costs and € 1M for SME grants[16] over two years. The first call of two corresponding calls had a budget of € 33M and closed on May 31, 2022. While this budget was sufficient to support about half of the European NCCs, just six of these NCCs saw themselves in a position to submit a corresponding proposal.

3. **Re-alignment of EU cybersecurity strategy and research**: The current *Horizon Europe* and *Digital* programmes come from a time without a war at the eastern EU border. The new geopolitical context imposes requirements for swift, co-ordinated efforts combining civilian and national defence cybersecurity measures. This kind of considerations are insufficiently reflected in the original programs and the road-mapping activities of the ECCC pilots (with the possible exception of CONCORDIA). These research programs and road-mapping activities were mostly technology- and policy driven, as is ECSO's strategic research agenda that predominantly took a technology and market-oriented perspective. As of mid-2022 and in the context of active warfare, the ICT infrastructures of EU member states find themselves under orchestrated attack. The priorities of cybersecurity research at EU and national level will need to be revisited in the light of this situation. Quite possibly, the clear separation of civilian and defence-related concerns that have been upheld as a matter of principle for all previous EU work programmes cannot be maintained in its current form.
   In the recent past, the creation of technical-roadmaps and research programmes was supported by well-coordinated input from ENISA, JRC, ECSO, and the four ECCC pilots. As the pilots come to the end of their lifetime, corresponding activities are handed over to the ECCC Strategic Advisory Board and its thematic working groups. However, the current immature state of most NCCs and their competence communities may limit their capability of contributing to technical agendas in the near future. An increase of requests from the defence and security community seems likely. However, the ECCN currently has no mechanisms for taking up and acting upon such requests.

4. **European market for cybersecurity products and services:** For more than a decade, the EU's efforts have been oriented towards combining market-driven and regulatory elements. They set out from the values of privacy and data protection, whose principles are spelled out in a legal framework that includes the GDPR, the NIS directive, and the Cybersecurity Act. This framework has been mapped to technology principles and development methodologies such as "privacy and security by design" or "secure supply and production chains". Adherence to these principles open up the possibility of certifying that ICT components and services having been produced according to best practices and implementing baseline security and privacy capabilities. Certification, in turn, may constitute a unifying element for the fragmented European market. It could also help to underpin the marketing of "Cybersecurity made in Europe", a label created by ECSO.
   The first round of research projects administered by the NCCs will exclusively be geared at national SMEs, which may be insufficiently equipped to support the EU's strategic efforts on consolidating the European market for cybersecurity products and services. To the contrary, NCCs may choose R&D topics primarily in support of national cybersecurity strategies that may only partially be aligned with EC policies. Consequently, R&D results may emphasize usability at national level while disregarding trans-EU deployment. SMEs may need to be convinced to adjust the production, validation and testing of components, to secure the production chain and to meet the procedural demands imposed by "privacy and security by design" principles. The size of the grants has to be chosen in proportion to the effort required to adjust development processes accordingly.

[16] European Commission: Deploying The Network Of National Coordination Centres With Member States. Call -- Cybersecurity and Trust Digital Europe Work Programme 2021-2022 (DIGITAL-2022-CYBER-02). 22 February 2022.
URL: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2022-cyber-02-nat-coordination

Chapter 3 ECCC and ECCN Support

Regulation (EU) 2021/887 includes very few constraints concerning the practical implementing of National Coordination Centres. A large variety of instantiations at national level is made possible thereby, which cannot easily be captured, classified and modelled in the context of a pilot. SPARTA maintained close contact with several institutions tasked with implementation of an NCC, but did not receive requests for supporting during the ramp-up phase. No details on NCC implementations were available throughout SPARTA's anticipated duration of 36 months, so the initial idea of experimenting with governance structures and processes in view of the ECCN was abandoned. SPARTA can offer little support with respect to interactions between national and international institutions. The main reason for this is that the collaborative and participative process of project formation bears little resemblance to a scenario where 27 national entities have full autonomy to structure their operations.

The effort required to establish a working relationship between the ECCC and the multitude of national coordination centres is reflected by the EC's current strategy to support the deployment of the NCCs. To this end, €60M have been earmarked, allocating up to €2M funding for each individual NCC. These grants can be accessed by submitting a proposal to the non-competitive CYBER-02-NAT-COORDINATION CfP, which has been issued exclusively NCCs. The EU grant has to be matched by the member countries, effectively doubling the amounts of €1M available for expenditure and another €1M for research grants to be distributed within the NCC jurisdiction, preferably to SMEs.[17]

The first of the two CYBER-02-NAT-COORDINATION calls was issued in February 2022. The low number of responses to the first call suggests that the implementation stage of most NCCs has not yet progressed to a point where such a proposal could be produced in the first place. Just 6 out of 27 designated NCCs applied[18]. The subsequent call will be issued in fall 2022. Since CYBER-02-NAT-COORDINATION is non-competitive, it can be expected that all remaining NCCs will submit proposals at this occasion, steady progress assumed. Once the corresponding contracts have been signed, NCCs have to get familiar with the intricacies of EC cascaded funding, including the processes for tendering, evaluating, reviewing and controlling research projects.

The organization, structure and processes of NCCs is likely to reflect idiosyncrasies and constraints imposed by that of their respective national governmental administrations. The provisional ECCC has to ensure a baseline of commonality, e.g. regarding admission criteria for the national cyber competency communities or minimal common catalogue of services that have to be provided by all NCCs.

SPARTA's model for pilot governance turned out to be very similar to the one adopted for the real world ECCC. During its final period, SPARTA's efforts therefore focused on demonstrating that its governance structure and processes were adequate for efficiently addressing its core objectives. The related tasks are similar to those that will have to be carried out by an ECCC: governance has to oversee multiple technical programs with very different scientific focus running in parallel, which have to be coordinated with transversal activities such as certification, education/training or roadmapping.

[17] European Commission: Deploying The Network Of National Coordination Centres With Member States, TOPIC ID: DIGITAL-2022-CYBER-02-NAT-COORDINATION. 22. February 2022. URL (retrieved 23.05.2022): https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2022-cyber-02-nat-coordination

[18] This information is based on personal comments of SPARTA consortium members who maintain close ties with the EC and their respective National Coordination Centres.

Political agreement on Bucharest as the physical location of the ECCC was reached in December 2020[19] and officially confirmed in January 2021[20]. Since then, the process for establishing the institution was mainly driven and facilitated by CNECT H.1. Preparatory steps included the nomination of the national contact points in order to form a provisional governing board with representatives from all participating countries. The first two Governing Board meetings took place in April and October 2021, and it first physical meeting happened in June 2022[21].

End of June 2021, the ECCC regulation entered into force[22]. By end of 2021, the Governing Board had published its rules of procedure and details for the staffing process[23]. In February 2022, the Chair of the board was elected[24]. From January to July 2022, 23 further decisions were passed by the Governance board, mostly concerning procedural and HR matters. As of July 2022, job advertisements for several key positions have been published. They concern the roles of the executive director, a finance and budget officer, a policy officer and two program officers. Application cut-off for is mid-September 2022, so it can be assumed that successful applicants will take up their work for the ECCC in the first quarter of 2023. This will be around the time when the beneficiaries of the first round of CYBER-02-NAT-COORDINATION CfP[25] on the deployment of National Coordination Centres will kick off their activities.

Of particular relevance for the future operation of the institution are the ECCC Single Programming documents (GB decisions No 2021/8[26] and No 2022/6[27]). They cover the work plan for the period 2021-2024, focusing on the implementation of operational functions of the ECCC (human resources, administration, legal framework, governance aspects, etc.) to acquire full operational capacity for fulfilling its mandate. To ensure a baseline of common procedures in future interactions between National Coordination Centres and their associated cybersecurity communities, the ECCC has

[19] European Commission: The new European Cybersecurity Competence Centre to be located in Bucharest, Romania. Press Release, 10.Dec 2020. URL: https://www.consilium.europa.eu/en/press/press-releases/2020/12/10/the-new-european-cybersecurity-competence-centre-to-be-located-in-bucharest-romania/

[20] European Commission: Decision (EU) 2021/4 taken by common accord between the Representatives of the Governments of the Member States of 9 December 2020 on the location of the seat of the European Cybersecurity Industrial, Technology and Research Competence Centre. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2021.004.01.0007.01.ENG&toc=OJ%3AL%3A2021%3A004%3ATOC

[21] European Commission: The European Cybersecurity Competence Centre: Governing board meets for the first time in Bucharest. Press release, 23. June 2022. URL: https://cybersecurity-centre.europa.eu/news/european-cybersecurity-competence-centre-governing-board-meets-first-time-bucharest-2022-06-23_en

[22] URL: https://twitter.com/InnoRadarEU/status/1409474392648736775

[23] ECCC Governing Board Publications: URL: https://cybersecurity-centre.europa.eu/governing-board_en

[24] Insight EU Monitoring: Cybersecurity: ECCC elects Pascal Steichen as Chair of its Governing Board. 17 Feb 2022. URL: https://portal.ieu-monitoring.com/editorial/cybersecurity-eccc-elects-pascal-steichen-as-chair-of-its-governing-board/370023?utm_source=ieu-portal

[25] European Commission: Deploying The Network Of National Coordination Centres With Member States. CfP DIGITAL-2022-CYBER-02-NAT-COORDINATION, 22 February 2022. URL: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2022-cyber-02-nat-coordination

[26] ECCC: Decision No GB/2021/8 of The Governing Board of the European Cybersecurity Industrial, Technology and Research Competence Centre Adopting the Single Programming Document 2021-2023 and the Statement of estimates 2021. 22. December 2021. URL: https://cybersecurity-centre.europa.eu/system/files/2021-12/GB%20decision%202021_8_ECCC%20SPD%202021-2023_budget%202021.pdf

[27] ECCC: Decision No GB/2022/6 of The Governing Board of the European Cybersecurity Industrial, Technology and Research Competence Centre: Adopting the Single Programming Document 2022-2024 and the Statement of estimates 2022. 16 March 2022. URL: https://cybersecurity-centre.europa.eu/system/files/2022-03/GB%20decision%20No%202022_6_ECCC%20SPD%202022-2024_Budget%202022.pdf

created a corresponding working group, and membership and registration guidelines have been published[28].

EB decision No 2022/6 lists following specific objectives of the ECCC (p10):

- Enhancing cybersecurity capacities, capabilities, knowledge and infrastructure for the benefit of industry, in particular SMEs, research communities, the public sector and civil society;
- Promoting cybersecurity resilience, the uptake of cybersecurity best practices, the principle of security by design, and the certification of the security of digital products and services, in a manner that complements the efforts of other public and private entities; and
- Contributing to a strong European cybersecurity ecosystem bringing together all relevant stakeholders.

These objectives are translated into four areas of activities for the upcoming period of work (p10):

1. Establishing strategic recommendations for research, innovation and deployment in cybersecurity, in accordance with EU legislation and policy orientations, and set out strategic priorities for the ECCC's activities;
2. Implementing actions under relevant EU funding programmes, in accordance with the relevant work programmes and the EU legislative acts establishing those funding programmes;
3. Fostering cooperation and coordination among the NCCs and with and within the Community; and
4. Acquiring and operating the ICT infrastructure and services required to fulfil its tasks where appropriate.

The following sections briefly discuss each of these areas in view of existing and required support provided by SPARTA, collaborative results of the ECCC pilots, European and national institutions.

3.1 Establishing strategic recommendations for RD&I and ECCC activities

The activity of providing strategic recommendations for RD&I is relatively well supported. The cybersecurity research agendas for HORIZON EUROPE and DIGITAL EUROPE are already defined for the next couple of years. Input from the ECCC will only be required in case of updates or extensions of these programs. Like all other pilots, SPARTA has produced a comprehensive roadmap for RD&I for the foreseeable future. The four roadmaps were consolidated and transferred to ENISA as contribution to an initial, mid-term cybersecurity research agenda for the ECCC.

The prominent role of ENISA for co-defining the priorities of future European funded cybersecurity research is underlined in (EU) 2021/887 which defines tasks, roles and interaction patterns in sections 35 and 42 of the preamble and articles 3.2, 5.2.c. Close cooperation between both agencies is also enabled by ENISA's permanent observatory role on the ECCC EB (Art 12.7). ENISA is holds a strategic advisory role (Art 13.4) regarding the strategic agenda and implementation of the ECCC, the adoption of multiannual programmes and annual programmes co-financed by EU member states. To support these activities, (EU) 2921/887 also envisages participation of ENISA representatives in the ECCC Strategic Advisory Group (SAG) as observer, advisor or expert (Art 18.5).

According to the same article, invitations for supporting strategic activities not only concern ENISA. They can also be directed at representatives of the EC and other European bodies[29] or members

[28] ECCC: Decision No GB/2022/7 of the European Cybersecurity Industrial, Technology and Research Competence Centre Governing Board on the Community membership and registration guidelines. 23 June 2022. URL: https://cybersecurity-centre.europa.eu/system/files/2022-07/ECCC%20Decision%20No%20GB%202022%207%20on%20Community%20membership%20guidelines%20WG1.pdf

[29] EU 2021/887 Art. 1.1 mentions the European External Action Service, the Directorate-General Joint Research Centre, the European Research Executive Agency, the European Research Council Executive Agency, European Health and Digital Executive Agency, European Digital Innovation Hubs, the European

from the cybersecurity community, which would include ECSO in particular. This organization has continued its work throughout the piloting process, continues to produce relevant studies on many aspects of the European cybersecurity ecosystem.

During the coming years, a number of serious strategic, research-political and contextual challenges will have to be taken into account by the ECCC and the ECCN. Their implementation phase coincides with the revision of the NIS directive and the adoption of the Cybersecurity Resilience Act. Neither of them were addressed by pilot activities, since they were outside their time horizon. SPARTA has produced relevant results for two major high-level initiatives, that is, the European Cybersecurity Certification Scheme and the Joint Cyber Unit, where several results and insights from SPARTA's T-SHARK sub-program should be applicable.

An important challenge concerns the establishment of productive interaction patterns with the network of national centres. The ECCC and the ECCN will have to reflect and pool national requirements at a strategic level with a European policy perspective. The Governing Board will appoint the Members of the Strategic Advisory Group, which is limited to 20 members (EC 2021/887, Art. 18.1). This means that not all member states can have a representative on this board to voice their strategic preferences and priorities.

There are options of pooling interests across different member states, but manoeuvres of this type may contradict the intended and desirable mode of operation of the Strategic Advisory Group. The authority of SAG members, in particular as far it concerns interactions with the cybersecurity community through working groups and public consultations, relies on being viewed predominantly as independent topical experts. The ECCC and its working group on the strategic agenda therefore has to ensure that all relevant input can be gathered without giving rise to politically motivated coalitions and compromises at the SAG level.

Since many aspects of cybersecurity are of horizontal nature, exchange of knowledge and best practices, the orchestration of ICT related activities, programmes, and the exploration of synergies across multiple DGs and bodies of the EC will be essential. The process for the ECCC becoming a member or observer in the EU Agencies Network has been launched. This would give the ECCC direct access to various EU institutions. It will maximize the options of the ECCC for soliciting input for strategic recommendations on European cybersecurity RD&I.

Given the preparatory work from the pilots and the availability of support from DG-CNECT, ENISA and other organizations, it is in a good position to cover strategy-related tasks once the ECCC has reached full staffing and financial autonomy. Care has to be taken, however, not to ignore strategic aspects that lie beyond the natural horizon of institutions of European scale.

The inclusion of actors representing ELSA perspectives is explicitly envisaged by (EU) 2021/887 and the recently adopted ECCC guidelines for community membership. Grass-root and ad-hoc initiatives from the social, legal and ethical (ELSA) spectrum may be highly agile and loosely organized. Importantly, global associations for enhancing security characteristics of Open Source components cannot become members unless they are seated in a EU country, and civil initiatives operating at the fringes of the cybersecurity ecosystem.

Due to their organizational structure, topical focus and political-geographic scope, neither global associations nor ELSA-driven initiatives are natural candidates for admission controlled national cybersecurity communities. Future interactions with entities of this kind will rely on targeted efforts in the context of the ECCC's strategic working group WG4. In the interest of separating concerns, it might be advisable to create dedicated sub-WGs for this purpose. This may simplify to co-opt relevant experts and initiatives that are not formally part of the ECCN and its community nexus.

Cybercrime Centre, the European Defence Agency as potential candidates for such cooperation. If relevant, the ECCC may also cooperate with international organisations.

3.2 Implementing Actions and EU Funding Programmes

As of mid-2022, the ECCC commands just rudimentary operational and administrative capabilities. Implementation related tasks are currently carried out by the EC on behalf of the ECCC. These tasks and activities will gradually be passed on to the ECCC once this institution becomes operational. The time required for this mainly depends on the speed of the staffing process. This gradual transition should not cause serious problems: over the course of several, research programs, DG-CNECT has gathered experience with procedural and administrative aspects of evaluating, executing and reviewing projects. It can therefore be assumed that the process knowledge required will be efficiently transferred to ECCC during its initial stages.

SPARTA has contributed to defining the qualification profiles for the managerial roles, as have the other pilots. The pilot cannot offer practical experience regarding the implementation of actions and programmes in "real time", though, since the design of the ECCC pilots did not allow activities of this type. With its pre-defined technical programs, SPARTA has proven that it is possible to govern thematically distinct projects with adequate performance evaluation, cross-program support for dissemination and a certain degree of synchronization between the different strands of activities. Compared to the nature and scale of the tasks required for operating the ECCC, SPARTA's prototypical results and insights are of limited value for guiding the day-to-day management of typical EU-funded sub-programs. Support for this line of tasks is therefore best provided by those EC entities that are experienced with practically implementing RD&I activities and programs at scale.

3.3 Foster cooperation among NCCs and within the Community

As of mid-2022, representatives for all NCC have been named, and several EB meetings have taken already taken place. This resulted in the creations of four ECCC working groups[30]:

- WG1 Community Membership
- WG2 NCC Reference Manual
- WG3 NCC Network Functions
- WG4 Strategic Agenda

Three out of four working groups (1,2 and 3) address core operations and functions of the NCCs and aspects of their interaction with the cybersecurity community, which indicates the overriding importance of these topics for during the initial phases of setting up the ECC Network.

A variety of factors will contribute to setting up bilateral and multilateral cooperations between specific NCCs. Geographical proximity and regional geo-political commonalities are likely to play a role. Incentives for cooperation may also arise from similarities in administrative structure and processes, national cybersecurity strategies, or the economic, political and social mechanisms employed for activating the national communities[31]. Some NCCs may focus on research-led activities, other ones may primarily be concerned with supporting their national cybersecurity industry, while still others may mainly be guided by advancing ICT security in areas that are relevant to national security objectives. Temporary "buddying" mechanisms between more and less mature NCCs could facilitate knowledge transfer. Permanent multilateral arrangements would allow sharing services and expertise between NCCs with different sizes and resources, thereby enabling trans-European Cyber Ranges utilizing an infrastructure provided by the ECCC.

In practice, the individual NCCs still differ widely in terms of maturity. The SPARTA pilot comprises of partners from 14 EU member states. Only one of them (Czech Republic) was in a position to

[30] Personal information from Martin Übelhör, DG-CNECT H.1, 3. May 2022
[31] see: G. Penchev et al: Governance Alternatives. ECHO Deliverable 3.2, July 2020. URL: https://echonetwork.eu/wp-content/uploads/2020/11/ECHO_D3.2_Governance_Alternatives_v1.0.pdf. The considerations for determining the main mission, directional outlook and organizational details for the ECCC presented by this study apply for NCCs by analogy.

submit a proposal for first round of the CYBER-02-NAT-COORDINATION CfP[32] call in spring 2022. Across the EU, less than 25% (6 out of 27 eligible NCCs) participated in this non-competitive call. The low level of maturity has undercut SPARTA's efforts to compile an initial structured overview about core characteristics of different NCCs in early 2022. Preparatory enquiries revealed that many NCCs were at the very beginning of their planning and were yet able to answer fundamental questions about staffing levels, utilization of inter-governmental services, or initiatives and programs for co-opting and interacting with their national communities. This indicates that the majority of NCCs do not have sufficient resources and bandwidth to draw practical benefits from cooperations amongst themselves at this stage.

In the near future, support for inter-NCC cooperation could be provided in a variety of ways. The establishment of rules and procedures applied by all NCCs will lower the barriers for cooperation as the level of common understanding and background increases. Corresponding activities are currently driven by the ECCC interim Executive Director, the Governing Board and its working groups. Guidelines have been produced concerning membership and registration to national cybersecurity communities produced by WG1[33] have been at the disposal NCCs since end of June 2022. The NCC reference manual (WG2) and the specification of network functions to be carried out by the NCCs (WG3) are work in progress. With high probability, both of them will remain "living" documents for some time, as they have to reflect, at least in part, practices that still have to be developed as part of the actual operation of NCCs.

The collection of proposals submitted in response to the CYBER-02-NAT-COORDINATION CfPs will provide the ECCC with detailed information about the organizational specifics, procedures and interaction types envisaged by the NCCs. On this basis, it should be possible to compile a structured overview of essential characteristics for the NCCs in all European member states in the first half of 2023. For individual NCCs, the availability of such an overview would simplify the identification suitable cooperation partners amongst their peers.

In addition to regular meetings of the Governing Board and the Strategic Advisory Group, workshops should be set up dedicated to information exchange between NCCs. These workshops should be targeted at the NCC's middle management, allowing them to share knowledge about internal processes and communication strategies, to identify possible programmatic synergies and to select suitable candidates for trans-national cooperation for specific areas of interest. Over time, these events could contribute to adjusting and extending the provisional NCC-specific decisions, reference manuals and scoping documents of the Governing Board and its working groups.

3.4 Acquiring and operating ICT Infrastructure and Services

The ECCC Work Plan 2022-2024 (ECCC decision GB/2022/6) anticipates the acquisition and operation of ICT infrastructure for supporting its tasks set out in Articles 4.2.d and 5 of (EC) 2021/887 and in accordance with the work items defined in Article 5.3.b. The scope and extent of ICT and services being operated under the responsibility of the ECCC is thereby limited to infrastructure components supporting its own staff and those enabling interactions with other EU institutions and members of the ECCN, in particular the NCCs.

For reasons of efficiency alone, substantial parts of the ECCC's work may utilize infrastructure and services already operated by the EC or other European institutions. For example, the processing of programmes, calls and projects not co-funded by national Member States are likely to be aligned

[32] European Commission: Deploying The Network Of National Coordination Centres With Member States. CfP DIGITAL-2022-CYBER-02-NAT-COORDINATION, 22 February 2022. URL: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2022-cyber-02-nat-coordination

[33] ECCC: Decision No GB/2022/7 of the European Cybersecurity Industrial, Technology and Research Competence Centre Governing Board on the Community membership and registration guidelines. 23 June 2022. URL: https://cybersecurity-centre.europa.eu/system/files/2022-07/ECCC%20Decision%20No%20GB%202022%207%20on%20Community%20membership%20guidelines%20WG1.pdf

with the existing services and processes supported by the EU portal. This also applies for co-funded programmes wherever their implementation is assigned to the ECCC. For programmes with cascaded funding (FSTP) and executed at national level, existing EC services for reporting and accounting are likely to be re-used and adjusted.

For an institution focussing on cybersecurity, the level of operational security of ICT operated under its responsibility should not only be on par with, but superior to that of other EU institutions. Successful attacks on the ECCC ICT would by necessity, call its technical competency and authority into question. The ICT should therefore be architected and operated according to rules and procedures that apply for other security-critical sectors of society.

The ECCC and ENISA will be the main EU institutions tasked with the support and implementation of the core elements of the EU Digital Strategy: digital sovereignty, certified security of ICT components and improved cybersecurity at European scale. Consequently, it could be argued that these two institutions constitute prominent tests-in-case for demonstrating the feasibility and the progress in their own realm of responsibility. This could be achieved by utilizing cutting-edge results in cybersecurity as part of their own infrastructure. The ECCC could cooperate with other EU bodies to drive deployment projects for infrastructures and capabilities at the level of European institutions in the context of joint procurement initiatives[34] synchronized with the ECCN and supported by corresponding RD&I programs.

[34] see (EU) 2021/887 recital 41

Chapter 4 NCC Support

The recent CfP for the Setup and operation of National Coordination Centres in Member States[35] is aligned with the high level objectives defined by Regulation (EU) 2021/887 and the EU cybersecurity policy, namely (1) capacity building at national and, where relevant, regional and local level, (2) cross border cooperations and (3) the preparation of joint actions. The CfP is non-competitive in that € 1M funding (to be matched by national contributions) is available for each of the NCCs in support of ramping up its operations over a period of 24 months. Another € 1M (also to be matched by national funds) will be made available as grants for SMEs at a funding rate of 75%. If the full size of the EC grant is requested, the overall budget for operational costs and third party funding will be € 4M. The specific objectives that have to be addressed NCCs applying for these grants are spelled out in the CfP as follows:

Strategic Tasks:

1. Contribution to the strategic tasks of the ECCC by taking into account national and regional challenges for cybersecurity in different sectors, cross-border cooperation and Joint Actions;
2. Finding synergies with national policies and strategies on cybersecurity and related RD&I
3. Coordinating activities with relevant European Digital Innovation Hubs

Community Services:

4. Acting as contact points at the national level for the cybersecurity competence community;
5. Assessing requests from national entities for becoming part of the Cybersecurity Competence Community; coordination of national competence community members;

Cascaded Funding for RD&I at national level:

6. Facilitation of the participation from civil society, industry, SMEs, academic and research communities in cross-border projects actions funded by EU programmes;
7. Supporting of stakeholders in their application phase for projects managed by the ECCC in cooperations with National Contact Points[36];
8. Implementation of actions for which grants have been awarded by the ECCC, promoting and monitoring involvement by relevant entities in ECCN and ECCC activities, promotion of relevant outcomes of the work of the ECCN and ECCC at national level;

Dissemination and Exploitation:

9. Strengthening the uptake and dissemination of state-of-the-art cybersecurity solutions (notably by SMEs);

The CfP ask applying NCCs to specify these activities further in their proposal. This requires some level of preparatory groundwork already carried out by the prospective NCCs. Judging by the relatively small number of six actual responses to the call, it can be inferred that in the majority of European member states preparations of this kind are still in early stages.

The CfP imposes no rules on the size of the support to a third party, nor the number, duration and topical focus for SMEs receiving such funding. The NCCs will first have to determine how many projects can reasonably be funded so that overhead costs for tendering, proposal evaluation, project reviews and financial controlling are kept at a reasonable level. A reasonable minimal size of such a project will also be determined by the overhead incurred by the SMEs applying for third party support. It should be kept in mind that the overall budget for all grants that can be handed out does not exceed € 2M, which is about the level of support of a single, mid-sized EU funded project. The complexity of

[35] see footnote 16
[36] E.g. those funded under call “HORIZON-CL3-2021-SSRI-01-03: National Contact Points (NCPs) in the field of security and cybersecurity”. 30 June 2021. https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2021-ssri-01-03

calls, proposals and controlling has to be kept at a minimum in order to make it a worthwhile effort for SMEs to apply for funding. Substantial upfront costs for proposals and low acceptance rates (which are typical e.g. for the process of applying for EU research funding) should be avoided in order not to discourage cybersecurity community members right from the outset.

The DIGITAL-2022-CYBER-02-NAT-COORDINATION CfP[37] on the deployment of National Contact Points for cybersecurity reflects the initial phase of the ECCN and the NCCs. The six beneficiaries of the first CfP will start their activities not before end of 2022. Those NCCs participating in the second call will take up their work half a year later. Given this timeline, the complete network of NCCs can be expected to be operational from mid-2025 onwards. Until then, NCCs will have to familiarize themselves with the procedural details of cascaded funding, EU research programs, calls for proposals, evaluation and monitoring, or synchronization with the ECCC and Digital innovation hubs. Unless opportunities for synergies with national research programmes exists, these objectives have to be achieved within 24 months and at a budget of up to €2M for operational costs and up to €2M funding to third parties to research projects.

4.1 NCC Structure and Functional Roles

While directive (EU) 2021/887 lists the tasks and processes to be supported by NCCs, it is silent regarding actual structure of these institutions, as they rely on peculiarities of the various national administrations. A purely functional perspective is represented by the clusters listed above and could e.g. be mapped to a structure with the following dedicated roles:

1. Strategic and operational management;
2. Contact point of contact for EC, ECCC, ENISA, as well as foreign NCCs;
3. Financial management, funding to third parties;
4. R&D, education and training;
5. Outreach and interaction with community members, in particular SMEs; (clerical) first point of contact for community members.

With adequate clerical, administrative and back-office support for each role, the core tasks mandated by NCCs could be covered by about half a dozen individuals. While the overall strategic and operational management could be assigned to any of the specialized roles (2, 3, 4, 5) as well, the level of expertise required for roles 2, 3, 4 and 5 is such that options of combining any of them are limited (dual qualification would be required). Depending on the number of projects managed by an NCC at any given time, the corresponding workload incurred might dictate full separation of roles.

Familiarity with cybersecurity issues will be required for roles 2 and 4, since interactions will, by necessity, include technical topics. Cybersecurity expertise would also be advisable for role 5 to support meaningful interactions with the community beyond the mere announcement of the availability of funding.

4.1.1 National Contact Point for EU institutions and Operational Management

As a national contact point, NCCs have to provide expertise and support strategic tasks set out in (EU) 2021/887 Article 5(2). Their interactions with members of the national cybersecurity community allows them to identify specific national and regional cybersecurity challenges in different sectors. Each NCC will have to analyse which of these challenges can be addressed through cross-border or trans-EU research projects and programs. Corresponding suggestions and proposals will then have to be communicated upstream through the ECCC's strategic and governance boards. Strategic objectives pursued by the EC will have to be communicated downstream, correlated with national strategies and R&D initiatives, and translated into programs and calls at national level.

[37] European Commission: Deploying The Network Of National Coordination Centres With Member States. CfP DIGITAL-2022-CYBER-02-NAT-COORDINATION, 22 February 2022.
URL: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2022-cyber-02-nat-coordination

NCCs will mainly be established as an integral or associated part of exiting national institutions that are already concerned with matters of cybersecurity. NCCs will thereby have insight into the R&D requirements of operational entities such as security operation centres (SOCs), emergency response teams (CERTs) and cybersecurity competence centres of academic, industrial and institutional nature, procurement agencies, or trusted suppliers. On the other hand, the sizes of the hosting national agencies surpass that of the NCCs by far. In this case, the resources and impact of NCCs could be viewed as rather limited in the context of the hosting organization. This will change once NCCs become more relevant, e.g. by extending their responsibility toward administering national R&D funds or if R&D activities become linked to procurement policies for public administration or critical infrastructures.

During the first 2-year period, NCCs have to acquire all capacities necessary to support the ECCC and to cooperate with peer institutions at national and European level. Corresponding indicators for success are e.g. the number of entities assessed and co-opted as members of the national cybersecurity community or the number and type of initiatives for widening the expertise of these members. Other indicators are the level of alignment and coordination of activities with relevant cyber policy goals at national and European level, or the number collaborative activities and synergies with other NCCs and with the ECCC.

4.1.2 Financial Management and Funding to Third Parties

If possible, the task of financial management should leverage back-office support from governmental entities already experienced with cascaded EU funding (FSTP). Support of this type could even be provided by entities that are familiar with the technicalities of FSTP grants without being genuinely concerned with matters of cybersecurity, Considerations of financial management should be applied for determining the optimal number of projects that should be funded to maintain a reasonable balance between administrative overhead and FSTP grants handed out to SMEs. With a reasonable number of projects funded in parallel, and sufficient back-office support provided, it should be feasible to administer the DIGITAL-2022-CYBER-02 related FSTP grants with one single full-time equivalents and adequate clerical support.

The duration anticipated for DIGITAL-2022-CYBER-02 related activities is 24 months. The financial support programs for third parties (FSTPs) will be mainly targeted at the uptake and dissemination of state-of-the-art cybersecurity R&D and solutions, specifically by SMEs. The definition of areas of activity, technical and non-technical activities such as training funded by DIGITAL-2022-CYBER-02 has to be carried out within rather narrow budgetary limitations of €2M per NCC. During project execution phase, progress and expenditure monitoring of FSTP funded projects has to be implemented to ensure overall compliance with the rules of the grant agreement and the procedures of project evaluation.

Under certain conditions, FSTP funding could contribute to overcoming financial obstacles at national level. High-risk initiatives so far lacking support from industry could be incentivized, including initiatives where national security benefits exist without being economically viable. E.g., there may be circumstances where public/private partnerships is a prerequisite for addressing a specific challenge, or in situations where R&D results or prototypes have to be supported for an intermediate phase while their markets in early stages. Once NCCs are established, they may gradually assume additional tasks, such as coordinating or managing nationally funded cybersecurity research programs, in particular where integration between EU and nationally driven projects, programs and strategies is required. The programmatic focus of the programs pursued by Digital Innovation Hubs should be monitored closely to detect potential overlaps and synergies with other areas of ICT research.

By staging multiple CfPs, e.g. in 6-month intervals, the design of later calls could benefit from experiences made in earlier ones, thereby enabling a gradual learning process and stepwise process optimization. This includes the quality of the financial management, which will be of central importance for assessing the NCC's in terms of efficiency, impact and sustainability.

4.1.3 R&D, education and training

Apart from its functional roles of supporting the ECCC and of administering EC funding through FSTP mechanisms, the main objective of NCCs is to help advancing cybersecurity research, development, innovation, training and education in their legislative realm. To gauge the relative positioning and competencies of national stakeholders in the context of European research activities will require corresponding technical expertise at NCC level as well as a detailed insight into the capabilities of the national cybersecurity ecosystem as a whole. During the initial NCC phase, particular attention will be given to R&D oriented SMEs and start-ups as potential beneficiaries of FSTP grants.

Initially, NCCs need to identify potential members of the national cybersecurity R&D community. Possible sources of information are e.g. the ENISA Cyber Atlas, past market studies commissioned by ENISA and ECSO, or the CORDIS database for organizations having participated in past EU or nationally funded R&D on cybersecurity (FP7, HORIZON 2020, HORIZON Europe, DIGITAL etc.). Additional sources may exist at national level, such as data collections from institutions tasked with cybersecurity, critical infrastructure, economic statistics at national level and national, regional or local registries. In practical terms, this activity will gather the contact details and types of expertise of prospective community members.

Research entities already experienced with EU funding will not benefit from the FSTP grants supplied through the NCCs in the near future unless they are SMEs. Further, the average size of FSTP grants could turn out to be too small to incentivize well-established academic or industrial research organizations, in particular larger ones. Still, European and national strategies do have to account for the current predominance of SMEs and micro companies in the EU's cybersecurity ecosystem.[38] Sharing knowledge and expertise between established and new players should therefore be actively facilitated by the NCCs, as an important strategic element for actively involving SMEs in R&D and the deployment of innovative solutions and services.

Given the large number of research areas in cybersecurity, it is advisable for individual NCCs to focus their calls on a small subset of topics. Over time, national research initiatives should be coordinated with those of other NCCs, which could be facilitated by the ECCC. Coordination may also be the outcome of continuous collaborations between NCCs which are facing common challenges, e.g. due to geopolitical or structural similarities.

The estimated shortage of almost 200.000 cybersecurity experts in Europe[39] underlines the importance of education and training, which has also been recognized by the EC[40]. All ECCC pilots have contributed preparatory work in this area[41], and the NCCs could play an important role in promoting and organizing campaigns for education, training and awareness at national level for and through their competence communities.

4.1.4 Community Support

NCCs are in charge of coordinating and interacting with their national community of stakeholders in cybersecurity, notably with regard to outreach and information activities related to ongoing programs and funding opportunities. The complexity of applying for FSTP funding should be reduced as far as possible. Still, expertise may have to be provided during the application phase. For organizations

[38] In 2019, 12000 SMEs and micro companies had a 75% share of the €25BN European cybersecurity market. See ECSO: Cybersecurity Made In Europe Label – Fact Sheet. November 2020.
URL: https://www.eurobits.de/wp-content/uploads/fact-sheet-label-cybersecurity-made-in-europe.pdf
[39] (ISC)2: Cybersecurity Workforce Study 2021, p25. October 2021.
URL: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx
[40] ENISA: Addressing the EU Cybersecurity Skills Shortage and Gap through Higher Education. November 2021.
URL: https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education/@@download/fullReport
[41] For SPARTA's contributions in this area, see URL: https://www.sparta.eu/training/

lacking experience with externally funded research, support may also have to be provided during the execution phase. The NCCs should provide a single point of contact and ensure the efficient routing of requests from community members to NCC coordinators in the appropriate field of specialization (technical, financial, training etc.).

A dedicated study on the national cybersecurity market and R&D landscape could be commissioned by NCCs to obtain a comprehensive overview of the national cybersecurity landscape. The results of these studies should be made available the ECCN to enable trans-national exchange of information and coordination of activities. It would advisable to collect data at national level in accordance with the structure of European databases and classifications, e.g., by employing the taxonomy of the ENISA Cyber Atlas. Mapping of the national landscape is a continuous process, so NCCs have factor in that the data is kept up-to-date. Updates should be propagated accordingly to European repositories such as the Cyber Atlas to enable ENISA, the EC and other European cybersecurity organizations and communities identify specific national expertise, topical clusters and suitable partners for trans-European research consortia.

4.2 Costs, Benefits and Added Value

During the initial phase, assigning half of the overall budget to administering research grants is justifiable, since the purposes of DIGITAL-2022-CYBER-02 is to ensure sufficient NCC capabilities within a timeframe of 2.5 to 3 years. In the mid- to long run, however, 50% administrative overhead are clearly out of proportion. The CfP puts the annual operating costs of an NCCs of around € 1M. Depending on national wages, this corresponds to a staff of six to ten full-time equivalents (FTEs), including equipment and expenditure for community oriented activities and travel. In case 20% administrative overhead is deemed acceptable, "economic viability" would correspond to €4M-€5M EU funding annually, facilitated through each NCC and targeted at national stakeholders. With 27 NCCs, this would translate to €120-€150M research grants *per annum*.

To put these figures into perspective: the EC's planned expenditure for cybersecurity for the two-year period 2021-2023 stands at €269M for DIGITAL EUROPE[42] and €134M for HORIZON EUROPE[43], corresponding to an annual budget of approximately €200M[44]. Under the financial assumptions made above, some 75% of the funding available for cybersecurity would be administered by NCCs. If the topic-oriented format of EC calls is to be maintained, a substantial level of coordination between the ECCC and NCCs as well as horizontal cooperation between NCCs will be essential. The national centres will have to cluster around themes, geopolitical commonalities, level of readiness and other commonalities to provide EU's research agenda.

For research entities accustomed to participating in EU funded cybersecurity research on a regular basis, the value added by involving their NCCs in applying for funding and carrying out research appears to be quite limited. These entities are familiar with the prerequisites for applying for EC grants, including the necessary interactions with their national contact points, the proactive tracking of EC calls. They possess the expertise necessary for writing high quality proposals and can leverage existing networks for optimizing research consortia. Initially, these organizations may see little advantage in sharing expertise and contacts with new and smaller players at national level

[42] Big Data Value Association: The Commission invests nearly €2 billion from the Digital Europe Programme to boost the digital transition. 10 Nov 2020. URL: https://www.bdva.eu/commission-invests-nearly-%E2%82%AC2-billion-digital-europe-programme-boost-digital-transition

[43] EC: Horizon Europe Work Programme 2021-2022. 6. Civil Security for Society. (European Commission DecisionC(2022)2975 of 10 May 2022)
URL: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2021-2022/wp-6-civil-security-for-society_horizon-2021-2022_en.pdf

[44] As stated in recent job advertisements. See e.g. ECCC: ECCC/TA/2022/05/SPO - Vacancy Notice for the position of Senior Policy Officer. 21 July 2022.
URL: https://cybersecurity-centre.europa.eu/system/files/2022-07/ECCC_Senior%20Policy%20Officer%20AD8_final2.pdf

entering the competitive field of publicly funded research. Initially, this may also limit the willingness to share this expertise with NCCs.

Eventually, the NCCs should be capable to offer incentives that counterbalance potential loss of competitiveness, notably by offering substantial research grants at national level. For the time being, however, all substantial sub-programmes on cybersecurity research will be managed by the EC on behalf of the ECCC. Until 2025, In comparison, the size of the grants handed out by the NCC may be considered as marginal by established research entities who already have a stake in EC funded cybersecurity R&D. Once the relevance of NCCs for the prospects of established research organizations becomes more perceptible, there will be little room left for such complacency. The relevance of NCCs could be increased by involving them in defining and implementing sub-programs or in evaluation and the review processes at European scale.

Chapter 5 Re-Assessment of D1.2 and D1.4

The following sections discuss assessment elements that remain relevant for the future operation of the European and national centres, networks and communities. The comprehensive list of assessment criteria derived from the original requirements of the CfP SU-ICT-03-2018 was updated and streamlined to reflect the evolution of the ECCC implementation since 2018. Aspect of continuous applicability are discussed with regard to the SPARTA deliverables D1.2 and D1.4 and in view of elements that could support the tasks and processes of the ECCC, the ECCN and the NCCs in future.

5.1 Contributions from Internal Assessment D1.2 for supporting the ECCC

Continued thorough validation of SPARTA's governance model in view of an evolving ECCC governance model was carried out until the political compromise on the ECCC directive. From then on, the structure and processes defined by (EU) 2021/887 became the reference point. SPARTA's organizational, functional, procedural, and operational aspects had been fully implemented at that stage and were validated practically on a daily basis in the management of the pilot. Monitoring. SPARTA's governance model (D1.2, Chapter 5) in view of assumptions made by the CfP SU-ICT-03-2018 became obsolete.

5.1.1 Evolution of task relevance over time

D1.2 assessed the scope of SPARTA's coverage of issues faced by a future real-world ECCC and ECCN. A preliminary list of topics and objectives had been included in the 2018 CfP for the pilots. The list below gives an updated view on the continued relevance of these topics (from a SPARTA perspective).

Nr		Task / Assessment Aspect	ECCC relevance	aspect addressed
1		Perform common RD&I in next generation industrial and civilian cybersecurity technologies applications and services	yes	**yes** *addressed by technical programs*
2		Common RD&I may include dual-use cybersecurity technologies, applications and services;, applications and services	yes	*no case of dual use*
3		Research on horizontal cybersecurity technologies	yes	**yes** *validation, cryptography,*
4		Research on cybersecurity in critical sectors (e.g. energy, transport, health, finance, eGovernment, telecom, space, manufacturing	yes	**yes** *T-Shark program: full spectrum cybersecurity*
5		Strengthen cybersecurity capacities across the EU and closing the cyber skills gap	yes	**yes** *given the size of the project, limited practical impact*
6		Support certification authorities with testing and validation labs equipped with state of the art technologies and expertise	limited	**partially** *by way of research on tools and processes for validation and practical validation effort for specific IoT-OS*
7		Scale up existing competences and demonstrated strengths to the European level	yes	**partially** *by way of cross-border and inter-pilot collaboration, limited structural or economic impact*
8		Take up relevant active digital ecosystems and public-private cooperation models	yes	**partially** *ECSO, friends & associates scheme, PPP model unsuitable in the context of the pilot design*
9		Solve technological and industrial challenges	yes	**yes**
10		Contribute to collectively develop and implement a Cybersecurity Roadmap	yes	**yes** *initial and updated roadmaps, contributions to trans-pilot, collaborative roadmap effort*

Nr		Task / Assessment Aspect	ECCC relevance	aspect addressed
11		Use the cPPP Strategic Research and Innovation Agenda on cyber security as a starting point	limited	**yes** *continuous interaction with ECSO*
12		Consider the relevant work of ENISA, Europol and other EU agencies and bodies in the creation of the roadmap and the execution.	yes	**yes** *(project design phase)* **partially** *(project execution phase*)
13		Set up a functional network of centres of expertise with a coordinating "competence centre"	yes	**yes** (4 technical programs) *limited transferability to practical ECCC-NCC setup*,
14		Assess various organisational and legal solutions for the Cybersecurity Competence Network, taking into account various criteria:	limited	**yes** *(project design phase)* **no** *(project execution phase*: *(discontinued in Y2)*
14.1		When assessing organisational and legal solutions for the Cybersecurity Competence Network, take into account the EU mechanisms and rules,	limited	**yes** *(project design phase*) **no** *(project execution phase***)** *(discontinued in Y2)*
14.2		When assessing organisational and legal solutions for the Cybersecurity Competence Network, take into account national and regional funding structures,	limited	**yes** *project design phase)* **no** *(project execution phase)* *(discontinued in Y2)*
14.3		When assessing organisational and legal solutions for the Cybersecurity Competence Network, also take into account funding structures offered by industry	limited	*project design phase:* **partially** *project execution phase*: **no** *(discontinued in Y2)*
15		Based on the above work, a governance structure should be proposed (i.e. business model, operational and decision-making procedures/processes, technologies and people)	no	**yes** *(documented in D1.1, D1.3, D1.5, assessed in D1.2, D1.4, D1.6)*
16		Governance structure, business model, operational and decision-making procedures/processes, technologies and people will be implemented, tested and validated in at least 4 demonstration cases involving all partners in the network.	no	**yes** *not directly transferable (lean management model pilot "program" structure does not easily translate into ECCC-NCC set-up*)
17		The demonstrators showcase the performance of the suggested governance structure, business model, operational and decision making procedures/processes, technologies and people and their optimization (in a measurable manner).	limited	**yes**, KPI-controlled, *not directly transferable: the lean management model pilot "program" structure does not easily translate into ECCC-NCC set-up)*
18		Clear milestones defined for the implementation of roadmap-related targets achievable by the end of the project	limited	**yes** *not directly transferable: less a pilot-centric, but more of a project-centric criterion*
19		The effectiveness of selected pilot governance structure is demonstrated by providing collaborative solutions to enhance cybersecurity capacities of the network	yes	**yes** *indicator for governance of single WPs / technical programs only, unless cross program synergies are expected*
20		Defined priorities (based on roadmap) to be addressed in the future by the Cybersecurity Competence Network.	yes	**yes** *preliminary inter-pilot roadmap consolidated by ENISA*
21		The effectiveness of selected pilot governance structure is demonstrated by by developing cyber skills (e.g. by looking at models to align cybersecurity curricula at graduate/post graduate levels; align cybersecurity certification programmes; classify skills with work roles).	yes	**yes** *unsuitable indicator for effectiveness of pilot governance, more suitable as indicator for governance of corresponding WPs/programs*
22	X	Ensure outreach, raise knowledge and awareness of cybersecurity issues among a wider circle of professionals, where possible in cooperation with EU and national efforts, spread the developed expertise.	yes	**yes** *publication / dissemination / exploitation*
23.1	X	Together with industrial partners and their cybersecurity research collaborators, collaboratively identify and analyse scalable (short/mid/long term[3]) cybersecurity industrial challenges in the selected sectors	yes	**yes** (*project design phase)* **partially** *(project execution phase)* *by way of involvement of consortium partners in roadmap process also open to associates, drawback: non-representative participation*

Nr		Task / Assessment Aspect	ECCC relevance	aspect addressed
23.2		Together with industrial partners and their cybersecurity research collaborators, demonstrate their ability to collaborate in developing appropriate solutions to solve critical challenges through (not less than four) research and innovation demonstration cases	limited	**yes** *by way of technical programs. Project-specific, not directly transferable to ECCC-NCC operations (e.g., no proposals / competitive tendering during the lifetime of the pilot)*

Table 1: List of potential tasks mentioned in SU-ICT-03-2018

As shown in the table, several of the tasks anticipated in the CfP proved to be unachievable or less relevant (the corresponding rows are highlighted in blue). D1.2 showed that during it ramp-up phase, SPARTA was in a position to address each single one of the potential tasks and objectives spelled out in the CfP. Over time, and as the legislative process progressed, the pilot arrived at a clearer picture which of these objectives could be realistically be addressed in a context of an EC funded project. This resulted to a prioritization of some efforts at the expense of downgrading others.

For example, it soon turned out that practical experiments that would change the governance structure and processes established by SPARTA would have unacceptable consequences for the efficient day-to-day management of the project. Consequently, SPARTA abandoned corresponding activities. The impact of this decision was minor, as the SPARTA's governance model turned out to be almost identical to the one for the ECCC as defined by (EU) 2021/887. In *practical* terms, this obliterated the necessity to cater for potential adjustments of SPARTA's structure and processes towards a very different ECCC governance. The corresponding assessment tasks (items 14-16 in the table above) could therefore be abandoned. KPIs and milestones defined for the demonstrators and technical targets (item 17and 18) did not require adjustments

In *theoretical* terms, information exchange in the context of the inter-pilot working group on governance revealed that questions of organizational alternatives (ECHO), social and regional span (C4E) and interaction with non-traditional stakeholders for EC-funded cybersecurity research (CONCORDIA) had been addressed by other pilots and did not have to be replicated. SPARTA's governance model, on the other hand, was geared towards determining new areas of innovation in cybersecurity, building up required expertise required through education and training, defining and carrying out mid-to large scale research programs, and assembling a network of suitable contributors to such programs. In view of SPARTA's achievements in all three areas of work, it can be concluded that its choice of governance structure and mechanisms proved well suited for the core objectives of the pilot.

As for the remaining tasks of reduced relevance: item 2 was not applicable since there was no instance of dual use in SPARTA. Supporting certification authorities with testing labs turned out to be a too ambitions objective to be shouldered; support was therefore confined to investigating and developing methods and tools for validation. The cPPP research agenda from ECSO (item 11) was indeed taken as a starting point to shape the initial technical agenda of SPARTA, but was then superseded by the pilot's own road-mapping results. Future, real-world research agendas for cybersecurity research in Europe are likely to take input from the working groups of the ECCC strategic board, ENISA and the JRC as main starting points. On the other hand, it is hard to gauge the future influence of ECSO on these agenda, which is the reason for ranking this point as "medium relevant". The same applies for item 23.2: the relative importance given to demonstrators in future EC funded cyber research programs it unknown.

5.1.2 Evolution of task relevance by category

In D1.2, the tasks listed in the table above were categorized into six thematic clusters. Tasks that turned out to be of lesser relevance over the duration of SPARTA appear in bold letters.

1. Generic governance (list items 1, 5, 9, 10, ***18***, 20, 22)
2. Technology and Innovation (list items ***2***, 3, ***6***,12)

3. Cybersecurity Competence Network (list items 8, ***11***, 13, 23.1, 23.2)
4. Demonstrators (***16, 17***, 21)
5. Assessment (***14, 14.1, 14.2, 14.3, 15***)

The listing shows that the relevance of generic governance tasks, technology/innovation and cybersecurity competence network remained relatively stable over time. In contrast, indicators related to the demonstrators (list items **16, 17, 18**) turned out to be inadequate for assessing the quality of SPARTA's governance model. In SPARTA, the program leaders were given autonomy to structure their technology related work. The main responsibility for the demonstrators thus lay with the program leaders. Apart from giving general guidance and tracking progress, SPARTA's technical director and the Executive Board did not intervene directly in steering these activities. All technical and demonstrator related work packages were completed successfully, confirming in retrospect this approach to pilot governance. It is an open question, though, whether SPARTA's streamlined, trust-based style of governance translates into the operational logic of an ECCC, the ECCN, or a NCC.

The most visible change in relevance occurred for governance-related tasks such as exploring organizational and legal alternatives in view of EU regulations, funding structures offered by industry or at national and regional level, and suggesting a governance and business model for the ECCC and the ECCN. In practical terms, the SPARTA consortium had accounted for all these factors when designing its prototypic governance structure. The model chosen reflected several educated "bets" on the most likely outcome of the political negotiations about the ECCC between the EU and the member states.

For the record, we note that the model finally chosen for the ECCC is almost identical to the one implemented by SPARTA. Prior to the finalization of (EU) 2021/887, the variety of possible governance models was too large to justify more than a basic level analysis being put into exploring their respective pros and cons. After the finalization of the directive, on the other hand, exploring alternatives became a mote exercise, since (EU) 2021/887 prescribed, from that point in time on, the future structure of the ECCC, the ECCN, and the NCCs.

NCCs are expected to have a ramping up period of more than two years. They should not be expected to be operational before end of 2024. Arguably, this is the earliest point in time when co-funding from national sources, industrial or risk capital schemes can be considered seriously. SPARTA decided not to continue related investigations during its last work period -- hence the reduced relevance of list items 14, 14.1, 14.2, 14.3, and 15***.*** To the best of our knowledge, the issue of complementary funding was neither explored by any of the pilots nor as an inter-pilot initiative. A corresponding study should be carried out in late 2025, when first experiences about the interactions between ECCC, NCCs, national contact points, and digital hubs are available.

While several tasks became less relevant due to changes of the pilot's operational context, some new aspects emerged that had not (and arguably could not) have been anticipated in the 2019 CfP. This regards adjustments following the actual outcomes of the negotiations on (EU) 2021/887 and various short-term requests by the EC for supporting preparatory efforts (roadmap, cyber atlas, interaction with friends and associates, inter-pilot working groups and synchronization). Resources freed up by discontinuing obsolete tasks could be utilized for addressing these new objectives.

5.1.3 Re-assessing recommendations for SPARTA's governance

D1.2 included a number of recommendations for deliberation at executive and strategic board level. They are revisited in this section in view of SPARTA's progress since 2020 and changes of the research-political context.

Main Findings:

- GC_M1(a) Further interaction with external entities occurred through a dedicated inter-pilot working group. Progress on a European certification strategy can only be achieved in a closely co-ordinated approach.
- GC_M1(b) Joint activities with European agencies and research programs was achieved through close interaction with ENISA and the other pilots, in particular on the first ECCC roadmap and the Cyber Atlas.

- GC_M1(c) The technical roadmap has been continuously updated and has been instrumental for giving input to the first ECCC roadmap.
- GC_M1(d) The provisions of (EU) 2021/887 were taken into account from early 2021 onwards. As a cross-border research project, SPARTA refrained from modelling interactions between ECCC and national entities (NCCs) (e.g. in regard to decision-making processes, the definition of CfPs involving cascaded funding etc.)

General Governance

- GC_G1: Re-allocation of funding for governance-related activities was not necessary.
- GC_G2: Over the duration of the project, SPARTA has developed a well-defined image with recognizable core competencies, systematically determining future areas research, designing corresponding programs, all-encompassing cyber security, validation and certification, education and training programs.
- GC_G3: No research on dual-use technology was carried out. Options of lightweight certification of software production processes (instead of certifying products and services) were investigated, which may influence development processes of Open Source software
- GC_G3: Interaction with other EC funded projects occurred, notably with the other pilots, but SPARTA did not enter into formal cooperations nor extended the consortium.

Governance Models

- GC_G5: SPARTA's T-SHARK program explored options of including operational capabilities in a competence centre at European level. These detailed investigation took place in the context of a future national CC (Lithuania), leveraging the advantages a central, coordinated national cyber agency with closely associated research partners. While the results of this program were remarkable, they relied in parts on the relatively low administrational complexity that can be afforded by a small EU country. The applicability of T-SHARK results for more complex scenarios such as the ECCC or the NCCs of larger member states would be a matter of further investigation.
- GC_G6: SPARTA did not adjust its governance model or processes in relation to the outcomes of (EU) 2021/887, given that in the current nascent state of the ECCC and NCCs, the power mechanics and balance between the institutions involved is mostly undetermined. In particular, this concerns joint decision-making processes about research agendas or about allocation of EC grants.
- GC_G7: By design, the pilot's program management and decision-making processes imposed minimal constraints and controls. They were mainly based on mutual trust between scientific peers. Therefore, they cannot be mapped directly to a real-world situation where one ECCC has to interact with 27 NCCs with potentially diverging interests-- even on a limited scale.

Horizontal Integration

- GC_I1, GC_I3: The level of integration between components produced within each of the four technical programs has been maximized and can be practically demonstrated. Mainly due to resource constraints, existing potentials for synergies could not fully be exploited.
- GC_I2: Direct interactions between the ELSA work package WP2 and the technical work packages WP4-WP7 by embedded scientist were made impossible by the outbreak and persistence of COVID. Corresponding research had to be constrained to theoretical analysis.
- GC_I4: The main interface to the Open Source ecosystem was SPARTA's consortium member SAP. The COVID situation has effectively blocked the pathways that could have been used by WP11 under normal conditions to initiate collaborative actions or training for this community (workshops, meetings in conferences etc). WP 10 organized two "business oriented" hackathons focusing on market oriented solutions relying on Open Source SPARTA results, as the source code for many of SPARTA's research results has been made public and can be taken up by complementary initiatives.

- GC_I5: WP11 mainly focused on curriculum development and had to align to the corresponding cross-pilot initiative. This limited the options for integration between the technical work packages WP4-WP4 and WP11 (training).

Continuous internal assessment activity

- GC_A1-A5: The result of D1.2 indicated close correspondence between pilot governance and the CfP requirements. The task of continuous monitoring and assessment was made part of operational project management as lightweight, KPI based replacement of an internal assessment with methods developed in D1.2.

In summary, there are three main concepts from the initial D1.2 assessment that continue to be of value for the practical context of the institutionalized ECCC and the NCCs:

D1.2 recommendations of continued relevance for ECCC, ECCN and NCC governance

The following main insights and results from the D1.2 assessment could be taken into account in practical context of the institutionalized ECCC and the NCCs

1. Methodically mapping political and programmatic goals to governance processes and performance parameters (as exemplified during the preparation of the DoA and D1.1 and subsequently assessed by D1.2);
2. Methodically locating synergy potentials between technical programs, that is, commonalities between projects that were not originally planned or anticipated
3. Continuously monitoring trends from industry, academia, standardization bodies, professional bodies and developer communities at international and national level in support for road-maps and topics of strategic importance;

5.2 Contributions from External Assessment D1.4 for supporting the ECCC

Early in SPARTA's second work period assessed by D1.4, the EC strongly encouraged inter-pilot co-ordination on common activities, namely security certification, governance principles, education/training programs and curricula, technical roadmapping, dissemination and interaction with the wider community. Near the end of that period, the National Cybersecurity Coordination Centres had been nominated by the EU member states, and the EC asked the pilots for input helping to define the main technical focus areas to be addressed.

From then on, one of the main functions of governance related work was to consolidate results, co-ordinate or merge these activities. In turn, all pilots had to re-evaluate the continued relevance of their activities -- within the constraints of their respective DoAs, with a view on de-duplication and complementarity of work between the pilots, and with reference to the operation of the future real-world institutions as laid out by directive (EU) 2021/887.

The D1.4 analysis concluded that tasks envisaged for the ECCC and the NCCCs in the preamble of the directive were well reflected in SPARTA's design and core objectives of fostering community engagement, building cybersecurity capacities, providing expertise, enabling coordination and co-opting stakeholders. Concerning the last point, future NCCCs will have to step up the game, using research-political and financial incentives that were not at the disposal of the pilots to engage organizations from industry, the research community, and the public sector. SPARTA's ELSA[45]-dedicated work package WP2 had considered options of involving a wider range of stakeholders from civil society. However, empirical work in this direction was made impossible due to COVID related constraints. These constraints also inhibited to intensify links to the Free and Open Source Software community as foreseen by preamble (EU) 2021/887, commentary 6.

[45] ethical, legal, and social analysis

5.2.1 Relevance and Applicability of Pilot Governance Results

The point-by-point analysis of the topical clusters of the directive carried out in D1.4 revealed a partial transferability of SPARTA's management and governance-related activities, results and methods. For 6 out of 11 types of ECCC, ECCN and NCC objectives, there is no or very limited transferability of SPARTA results, since the real-world operational characteristics are fundamentally different. This concerns the following areas:

- Governing Board representation, voting and veto mechanism
- Funding, involvement of and cooperation with other EC institutions
- National prerogatives for cybersecurity civilian and defence spheres
- Appointment and approval rights of the Executive Director
- Endorsement of and cooperation between NCCCs
- Interaction with other institutions, access to information and IP

In contrast, SPARTA can offer support in the areas of

- Defining mission, tasks, scope, Strategic Advisory Group
- Some responsibilities of the Executive Director such as monitoring and evaluation
- Inclusion of external participants in Board meetings
- Nomination for and appointment to the Strategic Board

The strategic planning process envisaged for the ECCC turns out to be roughly equivalent to SPARTA's road mapping process. The inter-pilot coordination on road mapping provides a template for the future work of ECCC Strategic Advisory Group task forces. The SPARTA consortium and its ecosystem is an example how to gather input for a strategic agenda a highly diverse group of contributors. Wherever possible and adequate, this level of diversity should be matched in future processes for defining ECCC and NCC programs.

There are commonalities between the role of the ECCC Executive director and those of the SPARTA technical director, such as implementing Governing Board decisions, tracking activities, or regular reporting on progress made towards mission and objectives. In particular, SPARTA's governance model included defined procedures for regular internal monitoring and evaluation. The pilot's KPIs, criteria and metrics used for assessing continued relevance and sustainability of activities will obviously be different from those of the future ECCC. However, and with some adjustments, elements of the pilot's assessment methodology may turn out to be applicable in the real-world context as well.

5.2.2 Applicability of Pilot Metrics for the ECCC / ECCN / NCCs

The analysis carried out in D1.4 established that only three out of seven ECCC result indicators mentioned in (EU) 2021/887 correspond to KPIs and criteria used for tracking the performance of the pilot. The indicators not matched by SPARTA KPIs concern objectives that were out of the scope for the pilot, specifically.

- The number of cybersecurity infrastructure / tools jointly procured,
- Access to testing and experimentation time across the Network and within the Centre,
- Access of user communities and researchers to European cybersecurity facilities, as alternative to similar resources outside Europe,
- An increase of competitiveness of European suppliers.

None of these criteria is applicable. SPARTA was not involved in procurement activities and did not provide testbeds or alternative cybersecurity facilities. As the pilot's technical activities have only recently ended and its results still have to filter through, SPARTA is not yet in a position to gauge the impact of its results on the competitiveness of European suppliers.

In contrast, the following ECCC result indicators do correspond to KPIs employed by SPARTA

- Level of contribution to next cybersecurity technologies, measured in terms of copyright, patents, scientific publications and commercial products;

- Number of cybersecurity skills curricula aligned and number of cybersecurity professional certification programmes assessed.
- Number of scientists, students, users (industrial and public administrations) trained.

There are well-known methods such as tracking the number of publications, the number of curricula considered for producing alignment proposals, the number of individuals participating in outwards-directed activities, or the number of tools produced for a particular purpose. It is therefore straightforward to translate these KPIs into ECCC result indicators.

D1.4 Recommendations of continued Relevance for ECCC, ECCN and NCCs Governance

The following insights from the D1.4 assessment could be taken into account in practical context of the institutionalized ECCC and the NCCs.

1. While there is some overlap of the success indicators for a pilot and an institutionalized ECCC and ECCN, they are far from equivalent. From a methodical perspective, it will be challenging to estimate the actual impact of ECCC activities on the European cybersecurity market or the cyber-threat level. Impact assessments relying on metrics such as number of publications or patents may prove to be of limited practical value for this purpose, as they do not reflect Europe's actual cyber-readiness.
2. The methodology of the external assessment included in D1.4 is, in general, transferable Key objectives, constraints and success indicators will have to be adjusted accordingly, though: there are fundamental differences between the modus operandi of a prototypic pilot implemented and the constraints of an EC funded project and that of real-world European and national institutions with financial and organizational autonomy. for assessing the activities of the ECCC and NCCs.

5.3 Adoption of Recommendations for Governance in SPARTA's Phase 3

During SPARTA's last period of work, decisions on adopting or disregard recommendations from assessments and reviews had to account for additional external constraints. This included the regulatory prerequisites imposed by (EU) 2021/887, requirements for cross-pilot coordination, and preparatory steps towards the practical implementation of the ECCC and NCCs.

From a high-level perspective, the majority of recommendations concerned

- governance and project management actions,
- internal coordination and information exchange between consortium activities,
- coordination with other pilots, ENISA, ECSO and initial ECCC activities
- outreach, dissemination and exploitation,
- strategic and practical details regarding SPARTA's technical contributions and tools,

For details on specific recommendations addressed, the reader should refer to document D1.5. As far as it concerns recommendations for governance, the idea of mapping aspects of the complex multinational ECCN structure to the SPARTA governance was dropped as practically infeasible. Concerning SPARTA's interactions with external entities, substantial effort was spent for cooperative work with the other pilots. Interactions with the Advisory Board were constrained to SPARTA final event.

5.4 Supporting and Sustaining Strategic Activities

SPARTA included a number of activities that were closely linked to governance in requiring closed coordination and interactions with external entities and communities. They served as instruments for

supporting high-level, general objectives and the strategic mission of an ECCC. With the exception of WP2, all of them concerned non-technical matters of transversal nature:

- WP2 – Roadmap instrument
- WP8 – Partnership instrument
- WP9 – Cybersecurity training and awareness
- WP10 – Exploitation and IPR
- WP11 – Certification organization and support
- WP12 – Dissemination and communication

We discuss which of these activities are of continued relevance and make suggestions how the relevant activities can be supported in a real-world context.

5.4.1 Roadmap Instrument

The initial SPARTA roadmap was geared towards the objective of strengthening Europe's digital sovereignty. Correspondingly, the process of road mapping first identified a number of major technical challenges, which were subsequently translated into thematic sub-roadmaps. The sub-roadmaps were updated in multiple iterative steps in view of new technological developments and in reaction to continuous input from consortium members.

During its final work period (M24-M41), SPARTA's mainly technology-driven perspective was complemented by those of the other pilots in the context of the inter-pilot Road-mapping Focus Group. This resulted in a consolidated input for to the first ECCC research program drafted by ENISA (currently non-public). This program is a significant step towards a cybersecurity research agenda dedicating to support digital sovereignty.

The SPARTA-internal as well as the inter-pilot road-mapping efforts combined mission-driven, top-down and thematically oriented, bottom-up approaches. The process as a whole strongly relied on open participation and co-operation of self-selection of contributors. This led to the inclusion of a wide range of perspectives and comprehensive input for specific topical areas. In our experience, indicate agile, flexible and open processes are highly suitable and efficient for addressing this type of tasks.

SPARTA's roadmapping exercises focused on purely technological challenges that have to be overcome in the interest of safeguarding digital sovereignty. However, it is increasingly recognized that cybersecurity crucially relies on non-technical factors as well. Similar efforts the context of the real-world ECCC will have to account for this by widening the scope of the investigation. The level of trans-disciplinary and trans-organizational collaboration required for this are far beyond the capabilities of the individual pilots and their Roadmapping Focus Group. More details on SPARTA's views and recommendations on this issue can be found in D1.5.

The roadmapping activity continues to be highly relevant. In future, they will be carried out by the Strategic Advisory group ECCC in the cooperation with the ENISA, the NCCs, and relevant administrative, academic and industrial bodies such as ECSO.

5.4.2 Responsibility Activities

From the outset, SPARTA emphasized the importance of responsibility related investigations. Corresponding activities on responsible innovation, ethical, social, ethical and legal requirements have been an integral part of the pilot's research agenda, addressing e.g. regulatory compliance, user acceptance at societal and individual level, ethical considerations and possible social implications.

In the meantime, we have witnessed e.g. an intense, privacy-related discussion concerning the design of COVID warning apps, a debate on the mixed blessings of remote management software and services that is still ongoing, and continued controversies regarding government influences on IT vulnerability management. Each of these examples points to the importance of including contextual investigations in cybersecurity research in order to identify and address relevant non-technical factors.

There have been many instances of tensions between cybersecurity strategies and demands of civil society, particular economic interests and national security, and it could well be argued that these tensions characterize this ecosystem as a whole. As a potential remedy, ELSA research supplies a range of tools for analysing the determinants and possible societal impact. If possible, research of this kind should be carried out ex ante. The recent past has shown, however, that priorities and relevant criteria may have to be adjusted quickly in situations of pandemics, military conflicts, partial breakdowns of global supply chains or civic conflicts. In situations such as these, ELSA-guided recommendations based on a small number of principles or rules and assuming a relatively static environment are likely to fall short.

Today, a comprehensive view on cybersecurity must also reflect whether protection mechanisms may entail undesirable dependencies and loss of sovereignty. Technological solutions for addressing older vulnerabilities may introduce new ones, and adequate risk analysis can be made more difficult in cases where traditional solutions with well-known levels of robustness are amended by IT based alternatives carrying unknown levels of risk. The strategic challenges faced by the ECCC and ECCN therefore go beyond defining and implementing appropriate technology driven research programs.

Public support for large-scale digitalization initiatives such as DIGITAL EUROPE can only be expected as long as the perceived advantages of ICT outweigh its drawbacks. This concerns not just the robustness of IT infrastructures and services, but also the public perception of individual and social (dis-) empowerment associated with ubiquitous ICT. Acceptance can also be predicated on the continued availability of traditional alternatives, be it as backup in situations of emergency, be it as a matter of autonomy, choice and freedom in a society increasingly mediated by ICT. The debate on responsible innovation and implementation of ICT in general and of cybersecurity mechanisms in particular approaches a point where not only concerns the "Hows" of protection mechanisms, but the "Ifs" of ICT and cybersecurity come under scrutiny.

Responsibility activities guided by research on ELSA and related disciplines should have a designated place in the structures, processes and programs implemented by the ECCN. This could be supported by co-opting relevant research groups and experts, by creating a dedicated working group of the ECCC Strategic Advisory Board, by including ELSA related investigations in programs and calls, and by research programs dedicated to this topical area. A balanced representation of perspectives could be supported by involving stakeholders who are not formal members of NCC-gated cybersecurity community.

5.4.3 Partnership instrument

SPARTA co-opted some 160 organizations in the area of cybersecurity, 44 of them as consortium members. The main objective of the instrument at the end of the pilot's lifetime was to encourage consortium members and individual members of its group of friends and associates to join and participate in their respective cybersecurity communities. The network of contacts created over the duration of the pilot will be utilized when it comes to setting up research consortia in future.

SPARTA's partnership instrument bears only limited resemblance with the ECCN community instrument, since there are fundamental differences regarding organizational set-up, admission process, functional role and incentive structures. This instrument has no continued relevance, since its function will be assumed by the NCCs and the ECCC from now on.

5.4.4 Cybersecurity training and awareness

SPARTA has designed, developed and piloted cybersecurity courses and trainings as well as tools for supporting education providers. In parts, this work was carried out in cooperation with other entities, notably ENISA, who became the lead partner for coordinating the development and compilation of a comprehensive course mapping and skills framework. SPARTA has contributed to

the initial programmatic document[46] defining the ENISA Cybersecurity Skills Framework[47]. Its final version will be presented in September 2022[48].

In support of ENISA's activities related to higher education, SPARTA gathered information on available education and training courses in Europe. The results feed into the CyberHEAD database[49,50] which helps EU students to tailor their cybersecurity syllabi.

WP9 has made efforts to ensure that the data that has been gathered will be kept up-to-date for some period beyond the project's lifetime. However, the long-term maintenance and sustainability of crowd-sourced databases like CyberHEAD remains an open issue that eventually has to be addressed by ENISA or the ECCC. Data should be updated at least twice a year, but tracking of available training, courses and educational programs across the EU is a tedious process requiring familiarity of native languages. This knowledge exists at NCC level, so these institutions could be tasked with providing bi-annual updates in a common format and language. This task should be included in the NCC service catalogue.

In cooperation with other pilots, SPARTA has prototyped access to external training material and tools through a portal operated by a Cyber Competence Centre. If the ECCC decides to mediate access to training resources are through a common infrastructure operated under its control, the responsibilities for maintenance and support will have to be clarified accordingly.

The European and National centres should be mindful that the provision of training and education is an essential enabler for interacting with the cybersecurity community. National specifics will have to be taken into account in many cases, which suggests the NCCs being the main drives of related activities. In this case, the ECCC would coordinate activities by setting up related working groups and hosting events like the recent ETACS workshop organized by SPARTA, where the CCN pilots, ENISA and NIST discussed the future development of Cybersecurity Training and Education in Europe.

5.4.5 Sustainable Exploitation and IPR

Intermediate non-technical results of SPARTA have been fed into the ramp-up process at various stages, notably in the context of governance (WP1), roadmapping (WP3), partnership and community support (WP8), education/training (WP9), and dissemination (WP12).

To facilitate the retrieval of assets and results to its researchers, SPARTA developed a management platform with prototypic services for assessing available resources, research-related data and results, for security requirement definition, privacy analysis, and IPR management. This platform was extended to support external entities as well, e.g. members of SPARTA's friends and associates program (WP8). The services have been made available through SPARTA's Joint Infrastructure (JCCI) in September 2021.

It should be noted that matters concerning the support of technical infrastructure operated by the ECCN, of exploitation and IPR management have not been addressed by any of the inter-pilot focus groups. At the time when the pilots were encouraged to co-operate, each of them had long since set

---

[46] ENISA: Cybersecurity Skills Development in the EU. Report, March 26, 2020.
URL: https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union/@@download/fullRepor t

[47] ENISA: European Cybersecurity Skills Framework. Draft Version, April 2022
URL: https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/ecsf-profiles-v-0-5-draft-release.pdf

[48] ENISA: ENISA Skills Conference, September 20-21, 2022. Agenda.
URL: https://ec.europa.eu/eusurvey/files/802cad16-e46d-4eb2-bfd2-9a0974d84f66/b2f829a5-a94b-4042-9646-1d5c83ca29e6

[49] Cyber Competence Network, 2021, CCN projects contributed to the ENISA CyberHEAD portal which helps students to choose cybersecurity programs.
URL: https://cybercompetencenetwork.eu/ccn-projects-contributed-to-the-enisa-cyberhead-portal-which-helps-students-to-choose-cybersecurity-programs/

[50] URL: https://www.enisa.europa.eu/cyberhead

up its individual processes and research infrastructures, resulting in path dependencies that thwarted coordinated efforts at later stages.

In any case, the introduction of a common infrastructure would be subject to explicit agreement between the ECCC and the NCCs, since individual NCCs are sovereign in their choice of structures, processes and technologies. In all likelihood, such efforts would be driven by a dedicated working group tasked by the ECCC's Governance Board. The continued relevance of SPARTA's results in this area would depend on its work into account at that stage.

5.4.6 Certification Organization and Support

Certification related activities were coordinated with SPARTA's technical research program CAPE that focused on methods and tools for IT security assessment, validation and verification. In this context, process efficiency and incremental methods for certification were identified as priority topics. This led to investigations and coordinated research on combining and integrating process and product oriented methods for certification documented in multiple deliverables of WP5 and WP11. From 2020 onwards, this was gradually extended toward to the research program HAII-T, although not at the same level of depth. While some experimental activities were carried out, coordination was mainly kept at a conceptual level.

During SPARTA's final phase, the result and insights of activities related to certification were communicated to national cybersecurity authorities in multiple meetings. The future EU Cyber Act is likely to task these authorities and so-called accredited conformity assessment bodies (CABs) with approving and issuing cybersecurity certificates, and it will be up to their judgement whether the processes developed by SPARTA will be used in practice. They will assess the merit of SPARTA's experiments on incremental product certification, and they will be in a position to compare the practical value of process versus product certification.

In the interest of continued relevance of its results, SPARTA has proposed model for collaboration between CABs and national certification authorities beyond the lifetime of the project. It would rely on a dedicated working group comprising of European CABs for sharing and promoting innovations related to cybersecurity certification. The introduction of cybersecurity certification at scale continues to be a core element of the European Cybersecurity Strategy The ECCC Strategic Advisory Group should therefore support the creation of such a working group.

5.4.7 Dissemination and Communication

While all ECCC pilots initially pursued individual strategies for disseminating and communicating their activities and results, these efforts were synchronised from 2021 onwards through an inter-pilot focus group. Building on the initial efforts of the pilots, dissemination and communication activities will be assumed by the ECCC and the NCCs. The ECCC has started to implement its own communication strategy in April 2021. It operates a dedicated web site with up-to-date news[51] and regularly informs about new developments via Twitter[52] and Instagram[53].

For SPARTA's long-term results, the reader should refer to the scientific papers and deliverables published during its lifetime. Dissemination will be of continued relevance for the ECCN, but its strategy is likely to differ substantially from that of the pilot. This is mainly due to the decentralized nature of the ECCN with NCCs playing a major role in communicating information to and from their national competence communities.

[51] URL: https://cybersecurity-centre.europa.eu/news_en
[52] URL: https://twitter.com/Cybersec_ECCC
[53] URL: https://www.instagram.com/cybersec_eccc/?hl=en

Chapter 6 Towards a sustainable ECCN

As elaborated in the previous chapter, SPARTA's main contributions for a sustainable ECCN regard the instruments of governance, roadmapping, social, legal and ethical responsibility, research program definition, support of the EU cybersecurity certification strategy, education and training and governance aspects supporting a technology-driven approach.

SPARTA's four technological programs continue to be of relevance for the EU cybersecurity strategy. Its work on assurance aspects for the Internet of Things contributes to addressing known gaps in the EU approach to IoT[54]. Activities on analysing threats and risks for Artificial Intelligence (SAFAIR) works towards improving the trustworthiness of AI, which is a prerequisite for employing this technology as a building block in future cybersecurity architectures as envisaged by the DIGITAL EUROPE programme[55]. SPARTA's research on continuous assessment feeds directly into one of the main objectives of the DIGITAL EUROPE cybersecurity program[56]. With regard to short-and mid-term applicability, SPARTA's T-SHARK program for 360-degree cybersecurity is particularly noteworthy. It addressed a number of topics related to cyber ranges in an integrated fashion, and its prototypic results are tested in the cyber-defence infrastructure of Lithuania under conditions of actual national defence.

Concerning the relation of SPARTA's governance model to that of the real world ECCN from D.1.4, some updates are in order to reflect the real-world efforts implementation in 2021 and 2022. Contrary to our assumptions, the establishment of the ECCC and the NCCs is likely to be a drawn-out process, and it may take until late 2025 before all NCCs have gone through the ramp-up phase supported by the DIGITAL-2022-CYBER-02 grants. For the near and mid-term future, cybersecurity research within the DIGITAL EUROPE program will continue to be managed by DG CNECT on behalf of the ECCC.

The DIGITAL EUROPE program will last until 2027, and its cybersecurity research has largely been defined already. It is conceivable that strategic adjustments will be needed, e.g. in reaction to new types of threats on protection mechanism. However, the ECCC nor the NCCs cannot reasonably be expected to influence the 2023-2024 agenda, and given the level of maturity that can be achieved for the institutions by 2024, their capacity of helping to shape calls for the 2025-2027 period is likely to be limited, in particular the impact of ECCC strategic efforts on trans-European sub-programmes.

For the time being, the EC can rely on its tried-and-tested methods of collecting input for defining the direction of cybersecurity research. These methods include the evaluation of past programmes, review of project results, dedicated information days and fairs, and collecting input from the stakeholders from the RD&I ecosystem. The ECCC will benefit from the pre-existing network and procedures and gradually acquire similar capabilities itself.

However, the new institutional setup will facilitate to involve stakeholders of the cybersecurity community that so far only played a minor role in the context of funded RD&I. This group of non-traditional players will now be mobilized by NCCs at the national level. Once effectively organized, their contributions will be gathered and channelled upstream through the working groups established

[54] DIGITAL EUROPE: New study finds gaps in Commission's approach to IoT cybersecurity. 8. September 2021.
URL: https://www.digitaleurope.org/news/new-study-finds-gaps-in-commissions-approach-to-iot-cybersecurity/

[55] European Commission: Annex to the Commission Implementing Decision on the financing of the Digital Europe Programme and adoption of the multiannual work programme - Cybersecurity for 2021 - 2022. Brussels, p13, 10.11.2021.
URL: https://ec.europa.eu/newsroom/repository/document/2021-45/C_2021_7913_1_EN_annexe_acte_autonome_cp_part1_v3_zCcOBWbBRKve4LP5Q1N6CHOVU_80908.pdf

[56] see previous footnote, p.25

by the Strategic Advisory Group. Thereby, the ECCC should obtain a more comprehensive view of the challenges, demands, and market situations in the field of cybersecurity.

The obvious way to efficiently utilize the ECCN would be to pool those interests of NCCs that strongly rely on coordinated RD&I at European level, to define and implement corresponding research, and to use FSTP funds level to disseminate the results at national level. This way, the FSTP funded activities managed by NCCs could become "transmission belts" for transferring EU funded cybersecurity RD&I into real-world applications and services. The amount of EU FSTP grants may turn out to be quite limited when compared with funding available at the national level. The FSTP instrument should therefore be complemented by better resourced, corresponding actions at national level. Combining research programs and procurement initiatives may help to generate a baseline of market demand and the timely uptake of results.

The double 75% majority voting mechanism foresees a blocking minority for the EC, which ensures the large-scale cybersecurity programs are strategically aligned with the strategy of the EU, could be endorsed. National voting powers on the ECCC Governing Board are predicated on the financial contributions of the EU member states to the programs. It is arithmetically possible that the EC and a small number of large contributors dominate decisions on future research directions. Care has to be taken to reflect the interests of countries with weak financial standing, but high exposure to cyber-attacks, as is currently the case for member states in the eastern part of the EU.

Compared to 2017, when the first ideas of a European Cybersecurity Competence Centre and network were presented, the determinants for an EU cybersecurity strategy have changed drastically. Cyber-attacks are increasingly attributed not just to organized crime, but also to government-sponsored entities. In addition to denial-of-service, information exfiltration and ransomware type malware, threats of attacks against industrial control systems employed in infrastructure and production has increased. A related class of attacks targets weakly protected IoT devices and their sensors and actuators. This happens at a time where the utilization of IT has made a leap due to the COVID-induced move towards remote work. Cybersecurity now also has to account for the provenance of components and for problems created by the global interdependencies of IT supply chains.

This and the recent geopolitical development suggests that we may enter a sustained period of de-globalization and re-regionalization with cybersecurity being treated as a matter of national and military security. Global dependencies and trust relations will be re-evaluated in this context, with the prevailing aim of more control over the production and operation of those parts of the ICT infrastructure that are deemed critical to keep societies intact. The ECCN could rapidly evolve into one of the core EU institutions devising an updated cybersecurity strategy towards more self-reliance and self-determination in the area of ICT.

SPARTA's governance activities, as well as those of its companion pilots, have done their best to adjust to these changes of context. The pilots' technical and non-technical activities have contributed to tackle some major challenges that have to be overcome for successfully implementing a cybersecurity strategy at European level. This was done within the constraints of a temporary research project with a limited lifetime, which means that some high-level aspects of strategic relevance for the EU could not be addressed. Notably, these regard institutionalized, transnational cooperations with research efforts from outside the EU and continuous working relationships with global cybersecurity alliances such as OCA or OpenSSF[57]. Future cooperations of this type and scale need to be driven by real-world organizations like ECCC, ENISA and other European institutions.

[57] For further details on the importance of these organization, see the corresponding chapter of SPARTA D1.4 on Open Source Security.

List of Abbreviations

Abbreviation	Translation
CCC	Cybersecurity Competence Centre
CCN	Cybersecurity Competence Network
CPPP	Contractual Public Private Partnership
DoA	Description of Actions (Project Plan)
EB	Executive Board
EC	European Commission
ECCC	European Cybersecurity Competence Centre
ECCN	European Cybersecurity Competence Network
ECSO	European Cyber Security Organisation
EDA	European Defence Agency
ELSA	Ethical, Legal, Social Aspects
ENISA	European Network and Information Security Agency
EU	European Union
KPI	Key Performance Indicator
NCCC	National Cybersecurity Competence Centre
OCA	Open Cybersecurity Alliance
OFE	Open Foundation Europe
OpenSSF	Open Source Security Foundation
OSS	Open Source Software
SB / SD	Strategic Board / Strategic Direction
WP	Work Package

List of References

Big Data Value Association: The Commission invests nearly €2 billion from the Digital Europe Programme to boost the digital transition. 10 Nov 2020.
URL: https://www.bdva.eu/commission-invests-nearly-%E2%82%AC2-billion-digital-europe-programme-boost-digital-transition

Cerulus, Laurens: 5 reasons why Bucharest won the EU cyber center race. Politico Pro, 11. December 2020
URL: https://www.politico.eu/article/5-reasons-why-bucharest-won-the-eu-cyber-competence-center-race/

European Commission: President Jean-Claude Juncker's State of the Union Address. Sep 13, 2017
URL: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_17_3165

European Commission: State of the Union -- Cybersecurity: Commission scales up EU's response to cyber-attacks. Sep 19, 2017. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_3193

European Commission: Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap. Oct 27, 2017
URL: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/su-ict-03-2018

European Commission: Speech by President-elect von der Leyen in the European Parliament Plenary on the occasion of the presentation of her College or Commissioners and their programme. Nov 27, 2019.
URL: https://ec.europa.eu/commission/presscorner/detail/en/speech_19_6408

European Commission: The new European Cybersecurity Competence Centre to be located in Bucharest, Romania. Press Release, 10.Dec 2020.
URL: https://www.consilium.europa.eu/en/press/press-releases/2020/12/10/the-new-european-cybersecurity-competence-centre-to-be-located-in-bucharest-romania/

EU: Decision (EU) 2021/4 taken by common accord between the Representatives of the Governments of the Member States of 9 December 2020 on the location of the seat of the European Cybersecurity Industrial, Technology and Research Competence Centre. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2021.004.01.0007.01.ENG&toc=OJ%3AL%3A2021%3A004%3ATOC

Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.
URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32021R0887

European Commission: The European Cybersecurity Competence Centre and Network moves forward: future Governing Board meets for the first time. Press release, 16 April 2021.
URL: https://digital-strategy.ec.europa.eu/en/news/european-cybersecurity-competence-centre-and-network-moves-forward-future-governing-board-meets

European Commission: Workshop of National Coordination Centres. Event publication, 25 May 2021
URL: https://digital-strategy.ec.europa.eu/en/events/workshop-national-coordination-centres

European Commission: Annex to the Commission Implementing Decision on the financing of the Digital Europe Programme and adoption of the multiannual work programme - Cybersecurity for 2021 - 2022. C(2021) 7913 final, 10.11.2021.
URL: https://ec.europa.eu/newsroom/repository/document/2021-46/C_2021_7914_1_EN_annexe_acte_autonome_cp_part1_v3_x3qnsqH6g4B4JabSGBy9UatCRc8_81099.pdf

European Commission: Deploying The Network Of National Coordination Centres With Member States. Call -- Cybersecurity and Trust Digital Europe Work Programme 2021-2022 (DIGITAL-2022-CYBER-02). 22 February 2022.

URL: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2022-cyber-02-nat-coordination

European Commission: Cybersecurity in Horizon Europe & Digital Europe. URL (last retrieved 2306.2022): https://cyberwatching.eu/sites/default/files/Cybersecurity%20in%20Horizon%20Europe%20Digital%20Europe_20210713.pdf

European Commission: The European Cybersecurity Competence Centre: Governing board meets for the first time in Bucharest. Press release, 23. June 2022.
URL: https://cybersecurity-centre.europa.eu/news/european-cybersecurity-competence-centre-governing-board-meets-first-time-bucharest-2022-06-23_en

Insight EU Monitoring: Cybersecurity: ECCC elects Pascal Steichen as Chair of its Governing Board. 17 Feb 2022.
URL: https://portal.ieu-monitoring.com/editorial/cybersecurity-eccc-elects-pascal-steichen-as-chair-of-its-governing-board/370023?utm_source=ieu-portal

European Commission: Deploying The Network Of National Coordination Centres With Member States. CfP DIGITAL-2022-CYBER-02-NAT-COORDINATION, 22 February 2022. URL: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/digital-2022-cyber-02-nat-coordination

European Commission: “HORIZON-CL3-2021-SSRI-01-03: National Contact Points (NCPs) in the field of security and cybersecurity”. 30 June 2021. https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2021-ssri-01-03

European Commission: Annex to the Commission Implementing Decision on the financing of the Digital Europe Programme and adoption of the multiannual work programme - Cybersecurity for 2021 - 2022. Brussels, p13, 10. November 2021.
URL: https://ec.europa.eu/newsroom/repository/document/2021-45/C_2021_7913_1_EN_annexe_acte_autonome_cp_part1_v3_zCcOBWbBRKve4LP5Q1N6CHOVU_80908.pdf

ECCC: Decision No GB/2021/8 of The Governing Board of the European Cybersecurity Industrial, Technology and Research Competence Centre Adopting the Single Programming Document 2021-2023 and the Statement of estimates 2021. 22. December 2021.
URL: https://cybersecurity-centre.europa.eu/system/files/2021-12/GB%20decision%202021_8_ECCC%20SPD%202021-2023_budget%202021.pdf

ECCC: Decision No GB/2022/6 of The Governing Board of the European Cybersecurity Industrial, Technology and Research Competence Centre: Adopting the Single Programming Document 2022-2024 and the Statement of estimates 2022. 16 March 2022.
URL: https://cybersecurity-centre.europa.eu/system/files/2022-03/GB%20decision%20No%202022_6_ECCC%20SPD%202022-2024_Budget%202022.pdf

ECCC: Decision No GB/2022/7 of the European Cybersecurity Industrial, Technology and Research Competence Centre Governing Board on the Community membership and registration guidelines. 23 June 2022.
URL: https://cybersecurity-centre.europa.eu/system/files/2022-07/ECCC%20Decision%20No%20GB%202022%207%20on%20Community%20membership%20guidelines%20WG1.pdf

ECCC: Decision No GB/2022/7 of the European Cybersecurity Industrial, Technology and Research Competence Centre Governing Board on the Community membership and registration guidelines. 23 June 2022. URL: https://cybersecurity-centre.europa.eu/system/files/2022-07/ECCC%20Decision%20No%20GB%202022%207%20on%20Community%20membership%20guidelines%20WG1.pdf

ECSO: Cybersecurity Made In Europe Label – Fact Sheet. November 2020.
URL: https://www.eurobits.de/wp-content/uploads/fact-sheet-label-cybersecurity-made-in-europe.pdf

(ISC)2: Cybersecurity Workforce Study 2021, p25. October 2021.
URL: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx

G. Penchev et al: Governance Alternatives. ECHO Deliverable 3.2, July 2020. URL: https://echonetwork.eu/wp-content/uploads/2020/11/ECHO_D3.2_Governance_Alternatives_v1.0.pdf

European Commission: Horizon Europe Work Programme 2021-2022. 6. Civil Security for Society. (European Commission Decision C(2022)2975 of 10 May 2022)
URL: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2021-2022/wp-6-civil-security-for-society_horizon-2021-2022_en.pdf

ENISA: Cybersecurity Skills Development in the EU. Report, March 26, 2020.
URL: https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union/@@download/fullReport

ENISA: Addressing the EU Cybersecurity Skills Shortage and Gap through Higher Education. November 2021.
URL: https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education/@@download/fullReport

ENISA: European Cybersecurity Skills Framework. Draft Version, April 2022
URL: https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/ecsf-profiles-v-0-5-draft-release.pdf

ENISA: ENISA Skills Conference, September 20-21, 2022. Agenda.
URL: https://ec.europa.eu/eusurvey/files/802cad16-e46d-4eb2-bfd2-9a0974d84f66/b2f829a5-a94b-4042-9646-1d5c83ca29e6

Cyber Competence Network: CCN projects contributed to the ENISA CyberHEAD portal which helps students to choose cybersecurity programs. 2021.
URL: https://cybercompetencenetwork.eu/ccn-projects-contributed-to-the-enisa-cyberhead-portal-which-helps-students-to-choose-cybersecurity-programs/

Digital Europe: New study finds gaps in Commission's approach to IoT cybersecurity. 8. September 2021.
URL: https://www.digitaleurope.org/news/new-study-finds-gaps-in-commissions-approach-to-iot-cybersecurity/

Digital Europe: How to secure the Internet of Things. June 2021.
https://digital-europe-website-v1.s3.fr-par.scw.cloud/uploads/2021/09/DIGITALEUROPE_Setting-the-standard_How-to-secure-the-Internet-of-Things.pdf

SPARTA Deliverable 1.1: Bootstrapping a CCN pilot. February 2020.
URL: https://www.sparta.eu/assets/deliverables/SPARTA-D1.1-Bootstrapping-a-CCN-Pilot-PU-M12.pdf

SPARTA Deliverable 1.2: Lessons learned from internally assessing a CCN pilot 2020. February 2020.
URL: https://www.sparta.eu/assets/deliverables/SPARTA-D1.2-Lessons-learned-from-internally-assessing-a-CCN-pilot-PU-M12.pdf

SPARTA Deliverable 1.3: Improving a CCN pilot. July 2021.

SPARTA Deliverable 1.4: Lessons learned from externally assessing a CCN pilot. 2021. July 2021.

SPARTA Deliverable 1.5: From assessing to supporting the future CCN. 2022. September 2022.