SPARTA

D11.4

Report on liaison with national cybersecurity authorities

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 / D11.4 / V1.0
Work package contributing to the deliverable	WP11
Due date	March 2022 – M38
Actual submission date	21st September, 2022

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

Abstract	This report briefly summarizes some of the interactions held between SPARTA and national cybersecurity authorities. It restricts itself to the publicly-transmissible part of these interactions.
Keywords	Roadmap, Education, Training, Policy

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

Editor

Florent Kirchner (CEA)

Contributors (ordered according to beneficiary numbers)

Geoffroy Hermann (ANSSI)

Disclaimer

Executive Summary

This deliverable summarizes non-confidential information exchanged with national authorities in the scope of the SPARTA project. It identifies key areas of involvement, such as certification, regulation, and organization. It proposes synthetic recommendations for the ongoing ECCC and NCCs ramp-up.

Table of Content

Chapter 1 Introduction 1
Chapter 2 Roles of national authorities in the European landscape 2
Chapter 3 Exchanges and recommendations 3
3.1 On the ECCC 3
3.2 On the NCCs 4
3.3 On (national) roadmaps 6
Chapter 4 Conclusion 8
Chapter 5 List of Abbreviations 9
Chapter 6 Bibliography 10

List of Tables

Table 1: ECCC recommendations 3
Table 2: NCCs recommendations 4
Table 3: Sample inputs from national roadmaps 6

Chapter 1 Introduction

Cybersecurity, perhaps more than most other scientific and technical fields, has strong implications on national sovereignty. Over the past decades, we've seen Member States evolve and grow new capacities to handle this domain, in the form of dedicated teams, specific divisions, and targeted agencies. Regardless of their scope, they have become *public authorities* in cybersecurity, and their role has been critical not only in operational matters, but also in promoting, surveying, and sometimes participating in research and innovation efforts.

Since its very design, SPARTA posited that the implication of national authorities would be a key element in building a relevant and efficient cybersecurity community. Some of them joined the SPARTA pilot as Partners, other as Associates. All of them came with, in mind, the knowledge that European cybersecurity was a key topic, and willing to play their role in this new perimeter. Their participation shaped the way SPARTA was bootstrapped and operated, brought in unique operational viewpoints and specific capabilities.

Throughout the life of SPARTA, numerous interactions have taken place between national authorities and other Partners, Associates, and Friends. In their nature, they have been quite diverse: person-to person meetings, interactions with specific Activities and Programs, sponsored presentations to private, European-focused sectorial working groups, just to name a few examples. Such interactions were boosted by two factors: (1) internally, the Monthly Workshops hosted Member State by Member State gave the opportunity to national authority representatives to attend the presentations and discussions, and engage if they so chose; (2) externally, the establishment of the ECCC and more specifically the designation and setup processes for NCCs has given rise to a number of interactions, not only on the state of play of European cybersecurity and the work done by the pilots, but also on specific recommendations and operational lessons learnt from SPARTA.

It should not come as a surprise to the reader, that a significant portion of interactions between SPARTA and national authorities are privileged communications. This report summarizes all non-confidential information exchanged.

Chapter 2 Roles of national authorities in the European landscape

Predicated on their internal priorities and organization, national authorities have positioned diversely in the European landscape. There are, however, several key points of interest for them in the current landscape, where their implication has been instrumental:

1. The topic of certification, an important element of sovereignty for Member States, and for which the European Cybersecurity Act requires EU-wide policy coordination. National authorities take part, for instance, in the European Cybersecurity Certification Group, which has held bi-monthly meetings since its launch in 2019.
2. The topic of regulation, in particular as part of the EU framework implementing EU's Cybersecurity Strategy for the Digital Decade, the Council Conclusions of 2 December 2020 and of 23 May 2022 or the Resolution of the European Parliament of 10 June 2021, spanning the NIS Directive and its NIS2 revision, the European Cybersecurity Act, and the Cyber Resilience Act.
3. The topic of National Coordination Centers, in line with the regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) and the Network of National Coordination Centres (NCCs) from June 2021. The designation of NCCs is creating new missions for national authorities, for which they are leveraging new cooperations within Member States and the Community.

Participation and cooperative work within SPARTA has helped in preparing and refining these points. Roadmapping in WP3, Community Activities from WP8, and Certification Activities from WP11 in particular have seen their engagement, as Partners and Associates, throughout the life of the project.

Chapter 3 Exchanges and recommendations

At pilot-level, four “Grand Principles” have been identified as recommendations for the whole ecosystem, and in the lead-up to the operationalization of the ECCC and Network for NCCs.

1. Enable **large-scale, multi-year research** that can transform whole industries and provide key instruments in the preservation and advancement of core European values of peace, human rights, democracy and rule of law
    a. Roadmaps gather the community’s creating thinking around **grand challenges and missions**. Associates help link the roadmaps to potential markets.
    b. Technical programs should be strongly mission-oriented, pursue **clear goals**, reward risk-taking and implement concrete measures to support failure-based learning
2. Establish and **reward leadership** at all levels of technical and transversal activities
    a. Focus on industry pure-players, aim at **targeted objectives**. Use Associates mechanisms to support wider-ranging impacts.
    b. Cultivate the engagement of a **variety of skills and profiles**, both on mission-oriented programs and in their transversal activities
3. Design and communicate **strategies** beyond the 3-year execution period into mid- and long-term challenges and missions, with explicit links to European values and societal expectations
4. Implement measures for **self-awareness**, including an Ethics Committee and independent evaluation mechanisms

From these principles, more specific recommendations have been derived, on the ECCC, on NCCs, and on roadmapping.

3.1 On the ECCC

From [1], “The European Cybersecurity Competence Centre (ECCC), together with the Network of National Coordination Centres (NCCs), is Europe’s new framework to support innovation and industrial policy in cybersecurity. This ecosystem will strengthen the capacities of the cybersecurity technology Community, shield our economy and society from cyberattacks, maintain research excellence and reinforce the competitiveness of EU industry in this field. The ECCC, which will be located in Bucharest, will develop and implement, with Member States, industry and the cybersecurity technology Community, a common agenda for technology development and for its wide deployment in areas of public interest and in businesses, in particular SMEs. The Centre and the Network together will enhance our technological sovereignty through joint investment in strategic cybersecurity projects.”

The table below summarizes SPARTA’s recommendations for the ECCC, resulting from its interactions with national authorities. Its contents, in turn, have been shared with national authorities expressing interest in them.

In this Table, RE/x denote a recommendation for NCCs, and the grayed lines the associated rationales.

Table 1: ECCC recommendations

ECCC recommendations	
RE/1	Introduce a European Competence Network as a first-class entity, with a mission to federate National Coordination Centres
	Networking is key, and cannot happen efficiently if just considered as a byproduct

ECCC recommendations	
RE/2	Mandate ECCC to recruit a wide diversity of experts to conduct its missions
	Based on propositions from NCC
RE/3	Mandate ECCC to consolidate NCC inputs on roadmapping, strategy, ELSA, capacities, and ensure their perennity
	Provide mission-oriented inputs and coordination to NCC following ECCC arbitrations
RE/4	Mandate ECCC to propose programs and activities opportunities, consolidate Community proposals, assessments and reporting
	Provide consolidated reporting to the ECCC and collaboration opportunities to the Community
RE/5	Mandate ECCC to conduct agile activities
	Avoid fixed, “fat cat” working group structure. Address emerging threats and opportunities, ethics and soc

3.2 On the NCCs

According to [2], “The Network of National Coordination Centres (NCCs) is constituted of 27 Centres, one from each Member State. They aim to boost research excellence and the competitiveness of the Union in the [field] of cybersecurity.” Broad requirements include:

- “the National Coordination Centres are public sector entities, or mostly State owned, or performing public administration functions”
- “they have the capacity to support the European Cybersecurity Competence Centre (ECCC) and the Network in fulfilling their mission”
- they “either possess or [have] access to research and technological expertise in cybersecurity”
- they “have the capacity to engage effectively and coordinate with industry, the public sector, the academic and research community and citizens”

The table below summarizes SPARTA’s recommendations for the NCCs, resulting from its interactions with national authorities. Its contents, in turn, have been shared with national authorities expressing interest in them.

Table 2: NCCs recommendations

NCCs recommendations	
RN/1	Leverage existing structures whenever possible: regional hubs, national and European associations
	Take advantage of community organization structures to minimize setup and operating costs
RN/2	Mandate inclusiveness and diversity, ensuring a minimum presence of academia, industry, grassroots, institutions, and citizen representatives at every level
	Inclusiveness and diversity needs to be a conscious effort

NCCs recommendations	
RN/3	Mandate activities around the dissemination of results, the use of common platforms, the transmission of recommendations, the popularization of strategies
	Make the community actors a vector to engage with European citizens
RN/4	Communities identify technical challenges to feed into national and European roadmaps
	A close proximity to operational constraints is key to effective roadmapping
RN/5	Communities propose subject-domain experts to lead specific programs and activities
	Experts can take the opportunity to lead their communities towards specific missions
RN/6	Communities propose multi-disciplinary contributions to programs and activities
	Fostering regional synergies without hampering European-wide cooperations
RN/7	Mandate NCC to build and maintain elements of roadmapping
	e.g. identified challenges, opportunities, etc.
RN/8	Encourage NCC to build and maintain elements of strategy
	eg. economic monopolies, infrastructure dependencies, threat actors, etc.
RN/9	Encourage NCC to build and maintain elements of ELSA
	eg. discovery, disclosure, etc
RN/10	Mandate NCC to build and maintain shared elements of capacity
	eg. evaluation platform, cyberranges, training, etc.
RN/11	Encourage NCC to distribute funding, perform performance assessments, and consolidate results
	Funding and assessment need to go hand-in-hand, and locality will help with agility
RN/12	NCC will interact with the Community of their respective perimeters to: - Recruit a wide diversity of experts to conduct its missions - Support proposals of subject-domain experts to lead programs and activities - Collect and organize Community feedback on its Roadmapping, Strategy, and Capacity missions - Dispatch dissemination activities to Community organization structures
	NCCs are the right level to implement pivotal functionalities beween the Community and the ECCC

Mirroring the previous Table, RN/x denote a recommendation for NCCs, and the grayed lines the associated rationales.

3.3 On (national) roadmaps

The work on national roadmaps has also helped feed SPARTA's roadmapping group, and hopefully the ECCC's priorities. National authorities have engaged in WP3 from this angle, foreshadowing the operation of the NCCs, consolidating inputs from various national groups and strategies, and contributing them to the European-level discussions. As an example, the Table below presents a summary of the inputs gathered by the French national authority ANSSI.

Table 3: Sample inputs from national roadmaps

Revue Stratégique de Cyberdéfense Technologies clés (publiée en 2018)

- Chiffrement ;
- Cloud ;
- IA appliquée à la cyberdéfense (a débouché sur le Grand défi) ;
- Conséquences physiques des cyberattaques ;
- Détection ;
- Informatique quantique ;
- Intégrité des composants électroniques ;
- GNSS et radionavigation.
- Open source ;
- Portefeuille de prestataires.

Grand défi « Automatisation de la cyber » (lancement en 2019)

- Réseaux dynamiques (convergence IT/OT, Cloud, mobilité, virtualisation) : cartographie, CTI, modélisation du risque, SOAR, etc. ;
- IoT (sécurité de la supply chain logicielle, détection locale, mise à jour sécurisée, etc.) ;
- Protection des petites structures contre la cybercriminalité (ergonomie, coût) ;
- Amorçage (start-up studio) ;
- Plateforme de données cyber à vocation européenne (dont AAP MVDC-CTI)

AAP Technologies Critiques 1 et 2 (programme de R&D technologique TRL 4-7 de la stratégie d'accélération nationale) (lancement en 2021)

- Développement de briques de sécurisation des outils de communication à distance et collaboratifs ;
- Développement de technologies de chiffrement innovantes (ex : ABE) ;
- Développement de solutions associant cybersécurité et sureté de fonctionnement à l'interface entre systèmes cyber et physiques ;
- Développement de solutions de cybersécurité pour la sécurité des grands événements ;
- Technologies innovantes visant à prévenir, détecter et remédier face aux ransomwares ;
- Mesure de l'exposition vue de l'extérieur des systèmes d'information ;
- Développement d'architectures innovantes de sécurité (IoT, Cloud, etc.) ;
- Développement de briques technologiques permettant de contribuer à la sécurité des terminaux mobiles ;
- Méthodologies innovantes d'analyses de binaires

PEPR (programme de recherche amont TRL1-4 de la stratégie d'accélération nationale) (lancement en 2022)

- Protection des données personnelles ;
- Sécurité des calculs ;
- Vérification de Protocoles de Sécurité ;
- Défense contre les programmes Malveillants ;
- Supervision et orchestration de la sécurité ;

- Architectures Sécurisées pour le Numérique Embarqué ;
- Améliorer l'évaluation de la sécurité des systèmes logiciels ;
- Protection des données multimédias ;
- Recherche et techniques d'exploitation de vulnérabilités ;
- Cryptanalyse de primitives cryptographiques à clés symétriques et asymétriques.

SPARTA has also collected specific recommendations from national authorities for the ECCC roadmap:

- Formalize the lifecycle (design, verification, update, monitoring, deprecation) method for the ECCC strategic agenda and the derived roadmaps
- Aim for a common European understanding of the objectives, ranging from the high-level goal to enhance strategic autonomy down to the fine-grained objectives of the Digital Europe and Horizon Europe work programmes.
- Include the specific objectives from the Digital Europe Programme, in particular in terms of technology acquisition and deployment, into the ECCC roadmap, to complement the inputs from the four pilots and ECSO. Identify sectors (e.g., in the NIS2 acceptance) and priority targets (SMEs, essential services operators, public entities, etc.) for the deployment of cybersecurity solutions.
- Identify emerging paradigms (e.g. zero trust, post-quantum, etc.) and decide whether the EU needs to address them, and how. In this exercise, be particularly mindful of key separating strategic opportunities and simple (but sometimes effective) deceptive marketing or inflated expectations.
- Contribute to a European industrial cybersecurity policy by identifying, from a market standpoint, the priority segments (e.g., detection, secure mobility, etc.) to derive key technologies and research and innovation actions in support to these technologies. This entails developing a thorough understanding of the European cybersecurity market.
- Fully leverage existing roadmaps, such as the roadmap from the pilot networks, or the investment strategies from the Member States. Elicit and supervise a follow-up to the "4 pilots and ECSO" synthesis document, with the aim to identify priority technologies.

Chapter 4 Conclusion

In liaising with national authorities, from the very inception of the pilot to follow-up actions in Member States after the end of the piloting phase, SPARTA has helped forge analyses and positions on key European policy efforts. This work has, in particular, helped bootstrap the organization and consultation topics of the NCCs. It will be sustained, in particular, in these centres, and within the relevant European working groups.

Chapter 5 List of Abbreviations

Abbreviation	Translation
ECCC	European Cybersecurity Competence Centre
ELSA	Ethical, Legal, and Societal Aspects
NCC	National Coordination Centre
NIS	Network and Information Security

Chapter 6 Bibliography

[1] https://cybersecurity-centre.europa.eu/index_en, accessed on 29/07/2022

[2] https://cybersecurity-centre.europa.eu/nccs_en, accessed on 29/07/2022