SPARTA

D1.3

Improving a CCN pilot

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

Deliverable type	Report
Deliverable reference number	SU-ICT-03-830892 / D1.3 / V1.0
Work package contributing to the deliverable	WP1
Due date	January 2021 – M24
Actual submission date	29th July, 2021

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

Abstract	This deliverable reports on how governance, R&D&I, community and exploitation activities have been monitored and improved during the first 2nd year of the SPARTA pilot.
Keywords	Policy capacities, Research governance, Mission-oriented innovation, Leadership management, Collaboration incentives

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

Editor

Florent Kirchner (CEA)

Contributors (ordered according to beneficiary numbers)

Thibaud Antignac, Augustin Lemesle (CEA)

Philippe Massonet (CETIC)

Jan Hajny (BUT)

Dirk Kuhlmann (FHG)

Marius Momeu (TUM)

Hervé Debar (IMT)

Alessandro Armando, Gabriele Costa (CINI)

Fabio Martinelli (CNR)

Evaldas Bruze (L3CE)

Bertrand Lathoud (SMILE)

Michal Choras, Marek Pawlicki (ITTI)

Gonçalo Cadete (INOV)

Reviewers (ordered according to beneficiary numbers)

Ana Ayerbe (TEC)

Raul Orduna (VICOM)

Executive Summary

This deliverable reports on the Governance improvements performed throughout the second year of execution of the SPARTA pilot.

The bases for these improvements included the internal assessment performed at M12, the first project review, and the related potential action points. They also benefitted from the tight and constructive interactions with the Commission, as was being refined the Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

From there, SPARTA proposed a modular governance framework, designed to address both in-pilot topics, and to provide reusable tools for out-of-pilot uses. In parallel, all SPARTA Activities and Programs continued their exploration of governance options within the greater framework, with leaders taking ownership for their perimeters, and yielding interesting returns of experience.

In fine, the SPARTA community has strongly evolved with regards to governance, making way for key facets of the future ECCC.

Table of Content

List of Figures

List of Tables

Chapter 1 Introduction

1.1 Purpose

This deliverable reports on how governance, R&D&I, community and exploitation activities have been monitored and improved throughout SPARTA's first 24 months of operation.

1.2 Context

The core mission for the European Cyber Competence Centre and Network (ECCC/ECCN) is to assist Member States in dealing with cyber-attacks[1]. On 8 June 2021, the Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres was published and defined the role of this future European body and its network; making the former a coordinator and clearing switchboard for directing funding for Cybersecurity research and development to National Competence Centres and the latter a distributor of this funding.

Although the Proposal for Regulation entitles the agency to procure and operate IT infrastructure it is highly unlikely that the ECCC will command genuine operative capabilities, e.g. for actively countering cyber-attacks. Instead, this agency will mainly be guided by mid-to-long term goals of improving cyber security in Europe through technology development, enabling industrial spin-offs and start-ups. In brief, the main instrument of the ECCC for furthering unified European approaches in cyber security is a support of research and technological innovation to strengthen European capacities in the field.

The Proposal for Regulation gives considerable autonomy to national cyber competence centres to govern their own affairs and communities. It remains to be seen whether this high level of national autonomy is compatible with aims of de-duplicating R&D efforts, where national competence centres and industries specialize in partial aspects of cyber security. First practical insight on this question will be gained during the initial phases of implementing the ECCC as soon as strategies of efficient work distribution and resource allocation have to be considered as there are traditionally conflicting requirements between regional specialization and digital sovereignty of countries. New and radical approaches are required to avoid inefficient duplication.

For many critical decisions, the voting arithmetic for the ECCC Executive Board grants a 26% blocking minority to the EC, board members, and weight of financial contributions. These stop gaps prevent free riding and ensure that important board decisions are always backed up by a substantial majority.

Given the relative autonomy of NCCCs to organize their own affairs now enshrined in the final Proposal for Regulation, the issue of mapping cybersecurity into national policies and institutional frameworks persists. Initially at least, there are likely to be stark differences between the member states' NCCCs. Over time, the initial variety of approaches might be narrowed down to a much smaller number of organizational templates that apply to clusters of NCCCs with similar organizational and procedural structures.

The ECCC will endorse national CCCs based on their expertise and capabilities. Regarding admission of organizations to the national cybersecurity competence communities, the ECCC plans to issue guidelines for safeguarding a common base level of admission criteria. However, the ECCC

[1] https://ec.europa.eu/commission/presscorner/api/files/attachment/854582/Cybersecurity.pdf

has no right for admitting community members; the policy for the actual admission is for the NCCCs to define and to execute.

The final version of the Proposal for Regulation now names civil society organizations as potential stakeholders and contributors. Organizations of this type could join the ECCC via national cyber competence networks and participate at a trans-European level in topical working groups. Since participation of civil society organizations is predicated on an accreditation by a national cyber competence centre, it depends on national policies whether such organizations are allowed to play a role. It is currently not obvious whether the topics addressed by the ECCN will mainly focus on technological issues, or whether other measures will be covered as well.

The Regulation foresees a permanent observatory and advisory role for ENISA. During the reporting period, this organization has made substantial efforts in support of a framework for security certification[2][3][4]. On the one hand, mandatory security certification continues to meet objections on grounds of costs, feasibility, and technical merit. On the other hand, the expanding threat landscape and the heightened vulnerability due to COVID-induced, ubiquitous online work demand measures for improving the state of IT security across the board, and certification is considered one option to address this problem.

Given ENISA's recent activities on cyber certification, it can be anticipated that future ECCC initiatives will be directed towards enabling voluntary and mandatory schemes of this kind. Like other pilots, SPARTA has dedicated activities in this area. If the ECCC decides to make this one of its strategic focal points, these activities could be channelled, into corresponding ECCC/ECCN initiatives, preferably as a cross-pilot effort.

The final Proposal for Regulation also includes provisions for initiatives concerning security and emergency services, critical infrastructure, the police, or the military. Admittance criteria for participation in corresponding strategic working groups could be defined by the working groups themselves, e.g., by introducing a kind of multi-level community membership, where some levels may mandate corresponding security clearances. Other elements of SPARTA, such as its efforts on road-mapping and corresponding technical focus areas, have already made it into the ongoing strategic planning process of the ECCC.

Like the rest of society, the project had to manage the impacts of the COVID epidemic[5], starting from its first review in February 2020. For the SPARTA pilot, it soon became apparent that pre-planned, DoA-defined activities were comparatively easy to continue, while re-adjustments and new activities turned out to be hard to initiate. This observation applied to the consortium as such and to interactions with external parties. Its main reasons are the constraints for physical encounters and exchange of personnel between institutions.

In order not to overwhelm the consortium members with additional demands, changes to the governance structure, processes and goals of SPARTA were kept at a reasonable minimum. This resulted a selective uptake of recommendations and suggestions. In practice, recommendations from EC reviews were addressed as fully as possible, while many internal suggestions from D1.2 were postponed or dismissed. With the exception of some non-critical delays, this approach kept SPARTA manageable and allowed to carry out its work as anticipated by the DoA.

1.3 Structure of the document

The remainder of this document is structured as follows. Chapter 2 gives an overview of governance reactions to external and internal recommendations. Chapter 3 introduces the concept of modular governance, and reports on governance aspects for Programs and Activities. The final chapter 4 presents the conclusions and an outlook.

[2] https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme
[3] https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme
[4] https://www.enisa.europa.eu/publications/cybersecurity-certification-market-study
[5] https://www.enisa.europa.eu/publications/year-in-review

Chapter 2 Internal and external recommendations

Through external reviews and its internal controlling process, SPARTA's governance has received a substantial number of suggestions on fine-tuning its activities with the requirements of a future European Cyber Competence Centre and Network. These suggestions are documented in the EC Review Reports following the M12 project review and in the M12 Deliverable D1.2 that assesses the SPARTA pilot from an internal perspective. The D1.4 assessment from an external perspective was carried out and finalized in parallel with this document. Its recommendations have yet to be acted upon and are therefore not discussed in this chapter.

2.1 Recommendations from M12 review

Table 1: Recommendations from M12 review

No.	Recommendation	Status
1	Some documentation and conclusions in deliverables suggest that the initial planning for a project of this size was wrong (though mostly related with identification of dual-use and data management plans). There is the risk that some other aspects were overlooked in terms of planning, and beneficiaries are encouraged to try to identify them or assess if risk measures to cope with them are required.	Continuously ongoing Risks and deviations are part of the quarterly IMR reports. As soon as the consortium identifies such wrong planning, risk measures to cope with the issue will be implemented.
2	It might be useful to consider a modular governance model or at least analyse how the model could work without some of the proposed parts.	Taken into account in Governance activity (WP1) This recommendation is taken into account in the governance-related activities to avoid to create strongly coupled elements, while still avoiding to create redundancies.
3	Some framework documents are currently presented as static and might be better serving if renewed regularly. Though it is not a perfect solution either, the usage of a wiki might be considered in the meanwhile, or at least describing its advantages or limitations in the context.	Taken into account in Exploitation activity (WP10) Preliminary attempts to use a wiki-based system have been performed. To overcome some limitations (e.g. automatic processing), a system based on MISP is being implemented, allowing to propose a federated solution to handle human-readable and machine-readable information around assets used during the project.
4	Beneficiaries must be careful to not work in silos and seek synergies between activities as well as between the H2020 cybersecurity pilots. Also finalize the advisory board.	Ongoing Synergies between activities are ensured through discussions during the EB and efforts put on internal communication (internal newsletter for instance). Synergies with other pilots are reached through inter-pilots focus groups

No.	Recommendation	Status
		(roadmap, governance, communication, cyber-ranges) and participation to Concertation meetings. The external advisory board is not yet operational due to delays in T11.2. Interactions with national authorities are long due to their global aim of remaining neutral. The setting for formal discussions with national authorities, through the External Advisory Board, is not yet ready. Discussions are thus ad-hoc.
5	Be more ambitious in terms of your publication goals and set better standards and criteria for what you consider good venues. Make this more transparent. Dissemination in other fora (media, niche publications, applied events, etc.) is strongly encouraged.	Continuously ongoing Updated the communication and dissemination Guidelines. These guides will be updated throughout the project, in particular taking into account the outbreak context.
6	It is fundamental to be more focused on added value and synthesis rather than reporting state of affairs. As a general comment for next deliverables is that the consortium should put more attention on properly describing the technical innovation derived from SPARTA programs. This should be enhanced by specifying the technologies that will be used, how they will be integrated, and the outcomes beyond SoTA solutions. Furthermore, more emphasis should be put in the integration aspects between SPARTA programs.	Continuously ongoing The consortium aims to submit high quality deliverables throughout the project. The consortium will therefore try to address this comment within all deliverables. Cross-program interactions are part of governance-level activities (especially in T1.2) to support mutualisation and synchronization between programs. For example, in the context of WP11, the relationship between certification criteria of WP5 and WP6 is discussed.
7	The “Cyber Risk Identification” per each Sector should be a continuous process. An Analysis model to forecast likelihood of the threat to happen and trending curve (increasing or not) is very critical and should be continuously implemented. Not only during audits for certification but should be treated as a continuous business operation.	T-SHARK (WP4) targets to deliver core components of the continuous Cyber Threat/Risk Identification and CS function is viewed as constantly ongoing dynamic process through two platforms: VAAS (comprehensive cyber threats visual analysis system) and T&AA (comprehensive threats and attacks analysis system). In SAFAIR (WP7), a risk matrix targeting ML cybersecurity has also been developed.
8	Some of the presentations performed during the on-site review meeting offered a higher-level executive view compared to the written deliverables and it is advisable to reflect that in future deliverables also.	Continuously ongoing The consortiums aims to submit high quality deliverables throughout the project. The consortium will therefore try to address this comment within all deliverables.

2.2 Recommendations from D1.2

Table 2: Recommendations from D1.2

Main Findings		Status
GC_M1	Four significant governance aspects are not fully covered yet. They all concern horizontal, co-operative and context-dependent activities: (a) Interaction with external entities and communities for validation and certification; (b) Potential joint activities with European agencies, external research programs and projects; (c) Roadmap updates to reflect new threats and cyber defence technologies; (d) Adjustments and extension of legal analysis to the (yet unknown) actual objectives of an ECCC / ECCN. It should be considered to track these four issues regularly and to include them in the list of risks to be managed.	(a) Interactions with external entities on validation and certification is a topic of T11.2. Meetings are planned with national cybersecurity authorities in the M24-M36 period on topics such as more efficient certification process and incremental certification to be materialized in D11.3. (Section 3.2.4). (b) In the second year of SPARTA, joint activities have been actively pursued and sustained with European agencies such as the JRC and the Atlas initiative. Focus group pertaining to certain aspects of the pilots have also been pursued in relationship with the other pilots, the EC and other European agencies such as ENISA for training and education activities and organisations such as ECSO for roadmapping for instance. We have also put into motion Letters of Support for other project proposals to initiate interactions with them while also fostering the creation of such proposals by the organisation of SPARTA Brokerage events. (c) The SPARTA Roadmap has been updated twice since its initial version - in January 2020 and January 2021. Its first update added 3 new challenges to reflect the new emerging technologies while its second added prioritization on the challenges, open-source aspects and Covid-related impact. In these updates, the opportunities and threats are reflected for the new technologies emerging in cybersecurity. (d) As mentioned, the precise objectives of the ECCC are not yet fully defined. However, some initial analysis of the legal context and possibility w.r.t. to cybersecurity and the ECCN has been performed in the scope of T2.2 and has been delivered in D2.3 in the meantime. The effort in that sense continue in the same scope for the third year of the project. More generally, these issues are of capital importance for SPARTA and are regularly monitored in the various bodies of SPARTA, (SD, EB, PC, RC …). Some of them are also

		covered by KPIs and already defined risks such as risk #24 (Lack of integration at European level).
General Governance		**Status**
GC_ G1	**Resources:** The average number of MMs allocated to governance for a EB or SD board member for all WP1 related tasks is 48MM. Just two of these members are substantially below average: FHG (35MM), and CETIC (26MM). Hence, most SPARTA partners involved in these boards have options for internally shifting resources towards core governance activities, including coordinative tasks. This information should be useful for realistically estimating options for adding functions, reinforcing horizontal activities or creating new ones, or collaborating with external initiatives.	The organizations represented at the EB and the SD correspond to Activity and Program leaders. Those partners are strongly involved in SPARTA, enabling them to implement decisions discussed during those boards. They also allow to have a distributed view of the execution of the pilot, feeding those boards with precise and direct information from the operations. Partners represented at those boards also have efforts in a series of transversal other activities in order to improve information sharing. Information collection from the stakeholders could be increased by establishing a stronger link with the Associates Council, though the Partnership Director, also chair of the Associates Council, is a member of both the EB and SD. (There is a typo in the figures: CETIC has 41 and FHG 37 PM in total)
GC_ G2	**Corporate Image:** Governance has to settle on a leitmotiv and a lucid set of easy-to-understand guiding principles, both indicating the general direction for SPARTAns, pilot associates, and the rest of the world.	The leitmotiv of SPARTA Governance has been defined early in the project in the form of its mission statement: “Shape the cybersecurity technologies required to establish and maintain a European Strategic Digital Autonomy”. While disseminated through various external presentation to SPARTAns, associates and the world, the guiding principles of SPARTA were later formalized in D1.1 Section 4.1.2 as a set of 5 clear and concrete principles taken from the proposal. These principles have also been disseminated through various channels in a standalone fashion to disseminate them. Additionally, in term of dissemination, the corporate image of SPARTA and its visual identity was settled in the beginning of the project and made available to all SPARTA Partners in the common project repository through a C&D Handbook, a SPARTA Workshop handbook, and various template for communication. As of early 2021, WP12 efforts of sharpening the profile of individual CCN pilots are complemented by trans-pilot efforts of developing a public understanding of the nascent ECCC, ECCN, and its national equivalents.

GC_ G3	**Consistency**: The following issues are points of potential controversies and may need addressing: (1) Research on dual use technology, interfacing with EDA or national defence. *For consideration:* refer this problem to Ethics Board. ELSA mediated discourse? (2) Implications of Certification for start-ups, SMEs, Open Source initiative. *For consideration*: consider options for advancing the case for verification and evaluation by other means than directly supporting the testing and validation labs of governmentally endorsed certification authorities. (3) Synchronization, cooperation, joint external initiatives with other CCN pilots. *For consideration*: No pilot can exhaust the whole range of topics, tasks, geo-administrative span, target audience, and governance models. Discourage "me-too" attitude, encourage and drive of differentiation, non-overlap, and carving out well-defined areas. (4) Liaising or co-operating with other projects, notably EC funded ones at early stages or in the pipeline enabling outreach. *For consideration:* Work Programme on Digital Societies, [13][14][15].	(1) Deliverable D14.1 has been submitted at the beginning of the project on the topic of dual use with the cooperation of the Ethics Board members. While at the time of this deliverable's writing none of the WPs expressed a potential dual use of their research, it might be pertinent to update this in the 3rd year of SPARTA with a clearer view of the researched performed and future research. (2) The implication of certification for start-ups and SMEs has been discussed in D11.1 which has been published at the same time as those recommendations while some aspects of certification for Open Source software were addressed in D11.2 published at M24. These aspects will continue to be assessed in the remaining time of the project both in WP11 and at Governance level. (3) The aspect of synchronisation between the four pilots has been a major focus point in this 2nd year of execution with numerous focus groups being created to synchronise the work done in the four pilots. This synchronisation was supervised by the EC and was taken in collaboration with external bodies such as ENISA or ECSO. It will continue during the remaining duration of the pilots and new focus groups will be initiated. (4) Two activities have been developed in the 2nd year of SPARTA to liaise with other EC funded projects. The first one being SPARTA Letters of Support and Expression of Interest to support projects in their proposal phase. The second one aims at supporting the creation of such projects with a brokerage event to discuss potential collaboration and project amongst SPARTA Friends and Associates.
GC_ G4	**Cooperations:** Consider co-operation with external initiatives and initiation of independent proposals to extend SPARTA's technological scope. E.g.: calls, projects and initiatives for Secure Society, securing Open Source components, Open Hardware, lowering the barriers to formal verification, changing the "geeky" image of verification into the next cool thing (motto: "programming without verification is something for script kiddies"), etc.	While SPARTA itself cannot expand the technological scope of its technical Programs as they were defined at launch for the duration of the pilot, SPARTA Roadmap aims at designating the most promising avenues for cybersecurity research and innovation. SPARTA Partnership organizes events with its Associates and Friends to foster the initiation of independent proposal through brokerage events. At the same time synergies are also created by SPARTA Partners involved in the proposal of other

		projects, such as with EU-HYBNET or Erasmus+ with REWIRE. On the program verification aspect, D5.3 in particular demonstrates that validation and assessment, when done on well-designed use cases, can be both useful and interesting to perform (incl. on open-source components).
Governance Models		**Status**
GC_ G5	**Alternate Models**: Consider developing a position statement on the following questions: Is it feasible and desirable to include operative capabilities as objectives for European CCNs? Should operative capabilities and research capabilities be administered by different European agencies (existing or newly created ones)? Should both types of capabilities be hosted by a single institution (ECCC / CCN)?	This lies beyond the scope of the SPARTA project, into European policy and the successful balance of sovereignty between Member States and the EU. While SPARTA is not equipped to address these questions directly, we note that findings and recommendations stemming from its Governance Activities might inform third-party studies on this topic. They will be documented as such.
GC_ G6	**Alternate Models / Contingency planning**: It is conceivable that a political compromise EC level will come out in favour of strong roles for National Cybersecurity Competence Centres (including powers to determine research directions and national beneficiaries) and limited powers for a central European hub. This may invalidate some of SPARTA's original working assumptions, and it will be a matter for governance to decide whether to adjust. In this case, it would fall upon WP1 and WP2 to prepare for such an outcome and to produce an organisational and legal contingency plan. This issue may have to be raised to pilot governance level and require a champion with a seat on the Executive and Strategic Board. Depending on the complexity of this task, a dedicated task force may have to be formed.	This alternative has been closely monitored throughout the start of the project, in relationship with all relevant stakeholders. If necessary, the steps suggested here would indeed have been deployed: adding a champion to the Executive and Strategic Board, and launching a taskforce on this topic. As this has not materialized, the development of adjustments and contingency plans was finally not necessary.
GC_ G7	**Alternate Models / Contingency Planning:** Consider experiments for emulating the structure and operation of National Competence Centres and clusters, and for developing corresponding interaction models. One	At this stage, this is addressed through two programs: (1) At governance model: T-SHARK governance model can serve as input for part of NCC activities, that must be validated after T-SHARK Stage #2 event

	or multiple of the WPs for the technical programs might serve as a conduit. The scenarios to be modelled can focus on Lithuania (WP4), Italy resp. Germany (WP5), France (WP6) and Spain (WP7). All work packages, but notably WP5 and WP7, could use some support from ELSA specialists to determine the respective institutional and legal framework.	on third week of 2020 December. Under this process, T-Shark can run NCC regional simulation on Baltic region. (2) At operational level: CAPE continued to function during Covid with only few perturbations. Different rovers could have been put in the same room, which did not happen. But code bases and tools sharing have been effective. Those use cases could most certainly be transferred to a NCC for sectoral leverage and maintenance and opened for research activities outside after the SPARTA pilot execution.
Horizontal Integration		**Status**
GC_ I1	**Technical Integration:** Clarify the desirable and feasible level of integration between the technical components and results produced by WP4-WP7. Clarify the achievable level of alignment between the four technical programs on the one hand and both WP8 and WP11 on the other.	WP4-WP7 technical results integration must be validated, which will happen in SPARTA third year. For CAPE in particular, D5.2 and D5.3 are already demonstrating joint work and integration. In the second year of SPARTA, WP11 has started coordination with HAII-T in addition of its cooperation with CAPE, participating in the HAII-T conferences. Cooperation with the other programs has only just started and is planned to encompass T-SHARK and SAFAIR in the third year. At the current time some interactions between Programs and Associates and Friends have been engaged through the use of the SPARTA JCCI and the tools integrated and available in it to Associates & Friends; for example Tecnalia's Smart Grid lab has been requested to be used in T-SHARK (WP4) by INOV and LIST as a member of the JCCI.
GC_ I2	**ELSA aspects:** The technical work packages WP4 and WP7 actively address areas of potential ethical, social and political concern. They are low hanging fruits for intensifying WP2 (ELSA related activities). Some effort should be invested to determine whether areas of particular ELSA relevance could be located in WP5 and WP6.	Initially during proposal phase, a SPARTA partner specialised in ELSA aspects has been included in each of the 4 SPARTA Programs. Those partners are also present in WP2 where they have space for more theoretical and generic activities. While due to the nature of threat intelligence and artificial intelligence, WP4 and WP7 are showing clear areas of cooperation with WP2, WP5 and WP6 are also under the continuous scrutiny of WP2. While some physical interactions had to be dropped due to Covid related constraints, other actions continued in the second year of SPARTA. In WP5, the most relevant ELSA aspect would be related to regulatory compliance and certification and D2.3 already underlines

		some of the working perspective on ELSA aspect in WP5. WP6 started a regular interaction with the ELSA program. In particular, dedicated meetings and discussions were carried to identify the ELSA-related topics in WP6. Among them, privacy issues received major attention. The activity is still ongoing and it will be finalized in year 3 (Section 3.3.2).
GC_ I3	**Synergies:** WP5 develops methods for infrastructure and "systems of systems" analysis. Could the results be beneficial for other technical WPs? E.g., are these methods applicable to analyse parts of the technical setup of WP4 or of task 11.4?	Technical programs (WP4, WP5, WP6, and WP7) architects will synchronize to identify synergy points between their activities during a workshop.
GC_ I4	**Open Source:** WP5 and WP6 may need support to engage with the Open Source spectrum in an active and sustainable manner. Could the scope of WP11 be extended by an activity targeting relevant Open Source communities? Are there individuals within the consortium or its group of associates who can and would act as champions?	In the second year of SPARTA, WP5 is actively engaged in open source, engaging the ECLIPSE community and integrating some of WP5 tools in it. At the same time, WP6 is actively engaged in RIOT, an open-source OS for IoT devices and on the redaction of the SUIT standard. In the scope of WP11, only some parts of certification were addressed for open source software. But WP11 is not currently taking into account the open source dimension in certification more broadly. Discussion on open source have already happened in the scope of WP3 Roadmapping activities and some reflexion at SD level will be initiated here which might reflect on all SPARTA WPs including WP11. Some discussion on interfacing two new globally oriented initiatives on Open Source security and certification are also discussed in D1.4. Related to exploitation, open source strategies in the software industry will also be a focus of WP10 (planned for the third year).
GC_ I5	**Hot Topics:** The combination and unified treatment of safety and security attracts increasing interest. Are there opportunities for co-operating with other CCN pilots, the aerospace industry, and providers for critical infrastructure?	This combination has been mostly developed in WP5, where we are focusing on connected vehicle, and in a very narrow scope, to be able to successfully deliver results in SPARTA timespan. It was judged a complex enough task as it is and no relevant activities were found in other pilots. Some links with other projects dealing with other critical infrastructures also exist here. This topic is part of the SPARTA Roadmap to ensure its continued presence among important cybersecurity challenges.

GC_I6	**Training**: The data from the questionnaire and our technical analysis suggest a huge disconnect between WP11 and the technical programs. Is this indeed the case? Is this intentionally so? Would it be possible and desirable to establish trans-WP links?	The interaction between WP11 and technical programs have been thought in an incremental approach in SPARTA. The first year has seen strong ties between WP11 and WP5 CAPE while in year two, HAII-T was successfully linked with WP11 in the form of regular conferences between both WPs. Finally, while T-SHARK and SAFAIR revealed only little needs for certification after some initial contacts, the interaction will be continued and increased in the last year of SPARTA (Section 3.2.4).
Continuous Internal Assessment for Pilot		**Status**
GC_A1	**Measurability:** To ensure proper progress tracking for governance (e.g., regarding those aspects that yet to be addressed in full), internal assessment could carried out more frequently, e.g. by combining internal assessment with the quarterly or bi-annual WP13 management reports.	In the scope of SPARTA the resources necessary to carry out such a frequent assessment were not set aside at proposal phase. This would however be a matter for consideration in another similar scope to reserve such resources. This would however requires higher resources dedicated to governance aspects, to balance with the operational ones.
GC_A2	**Network analysis:** The methods developed by T1.4 so far only apply at task and WPs level, but do not account for individual contributors. They are too coarse to produce tangible evidence for the existence of network-typical phenomena such as horizontal interactions, dependencies, or build-up of social capital. Are complementary methods required here? Should T1.4 type assessment monitoring be carried out more often than on an annual basis?	Individual contributors should not be part of the analysis of the governance and need to be handled with caution and respect of any data protection issue. However, interactions inside SPARTA as an organisation might be of interest if not exploited. Complementary methods can be discuss to improve the granularity of the analysis. However similarly to GC_A1 the resources necessary for such a fine grain monitoring or for a more frequent monitoring were not set aside in SPARTA at proposal phase and this might be a matter of consideration for a similar scope.
GC_A3	**Data Mining / Ethics:** Governance assessment could benefit from including data from the project management infrastructure, with a good chance to improve the quality of future internal assessments. In this context, it should also be considered to upgrade the current 40-seat license for the management support service *Stackfield* to a corporate one. This would enable statistical functions that are currently unavailable and would support the T1.4 internal pilot assessment. However, the stated purpose of internal mailing lists, the document repository and the notification and conferencing	The Stackfield tool was dropped, due to other limitations in the SPARTA context, in the scope of the management and collaboration infrastructure to be replaced by NextCloud. If similar tools as those mentioned were to exist for NextCloud the first point would indeed be to discuss the issue with the Ethics Committee. Until now, any solution of the sort to monitor the NextCloud infrastructure was not pursued.

	system is to support the SPARTA partners in their work, not to deliver data source for an assessment purposes. We suggest presenting this issue to Ethics Committee.	
GC_A4	**Risk Management:** The T1.4 metrics for achieved objectives and the WP13 oriented metrics for the risk of *not* achieving them is very loosely coupled, if at all. In co-operation with partner INOV, T1.4 could be tasked to investigate whether there are industry-strength methods that offer better granularity, closer coupling, and an integrated view on progress vs. risk. Pilot governance may consider including those objectives that are currently incompletely covered in the list of managed risks.	In the second year of SPARTA, T1.4 has added the KPIs as part of the internal periodic reporting alongside the risks. While only giving a rough indicator of progress this puts both risks and achieved objectives in the same scope.
GC_A5	**Capability Atlas:** The internal assessments D1.2 and D2.2 could form the basis of future directory of SPARTA capabilities, supporting governance and stakeholders in building dedicated task forces.	A directory of decision-making processes, governance structures, role specifications, and other parts related to governance in SPARTA could indeed benefit to future subsequent initiatives. WP1 deliverables will constitute the core of this documentation, made publicly available after their acceptance throughout the project life. This atlas is also supported by the JCCI which acts as a structured repository of cybersecurity platforms;

Chapter 3 Modular governance framework

During the course of its second year, SPARTA continued its work to conceptually and operationally organize the activities of a Cybersecurity Competence Network around a modular governance. This Chapter describes the CCN Structure proposed in Section 3.1 and the way this structure has been instantiated as transversal activities in Section 3.2 and as scientific and technical activities in Section 3.3. Material related to assessment activities will be integrated to D1.4 (Lessons learned from externally assessing a CCN pilot, PU, M27[6]).

3.1 CCN structure

In order to provide a governance to strengthen the European cybersecurity capacities, SPARTA has reinforced the structure of its activities to establish a modular governance. Four governance levels have been identified:

- **Network**: this level corresponds to the high-level activities aiming at organizing the other activities and the information flow with other institutional organizations;
- **Transversal**: this level corresponds to the activities related to partnership, training and awareness, exploitation, certification, dissemination and communication;
- **Scientific and technical**: this level corresponds to the activities related to scientific and technical activities (roadmap, R&D&I programs);
- **Assessment**: this level corresponds to the lower-level activities aiming at organizing the assessment activities.

Orthogonal to these four levels, five different kinds of processes have been identified:

- **Perform**: denotes the set of activities related to the execution of main objectives;
- **Monitor**: denotes the set of activities related to the control and monitoring of the activities;
- **Improve**: denotes the set of activities related to the continuous improvement of the way activities are executed;
- **Synchronize**: denotes the set of activities related to the internal and mutual information, good practice, and feedback sharing as well as synchronization between the activities;
- **Liaise**: denotes the set of activities related to the information sharing with and retrieval from external activities.

The three first kinds of processes are inspired from the PDCA (“plan”, “do”, “check”, “act”) continuous improvement quality instrument. While the “plan” is, implicitly, the initial basis from which SPARTA has been launched, the “do” corresponds to the “perform” process, the “check” corresponds to the “monitor” process, and the “act” corresponds to the “improve” process. The two last kinds of processes are designed to make information flow internally (“synchronize”) and externally (“liaise”) in order to ensure a proper coordination between the activities themselves on one hand and both the activities and the outer world on the other hand.

These processes are subdivided into subprocesses, which are projected onto the level to which they correspond, in order to ensure their cross-level consistency. Those instantiations refer to SPARTA-specific concepts. For instance, one of the subprocess of kind “perform” is “drive SPARTA strategy” at the network-level, and there are subprocesses “propagate strategy to Activities” and “propagate strategy to Programs and Roadmap” at the transversal, technical, and scientific levels. Those three specific subprocesses refer to the same “strategy” element.

In order to concretize the subprocesses and to improve their traceability, artefacts have been identified and constitute well-defined and actionable elements around which the subprocesses function. Finally, a frequency at which the subprocesses should be triggered is also set.

[6] Amendment request pending.

In the rest of this Chapter, processes related to the network level will be shown in Section 3.1.1, those related to the transversal level in Section 3.1.2, those related to the scientific and technical level in Section 3.1.3, and those related to the assessment level in Section 3.1.4.

3.1.1 Network level

Table 3 below shows the processes, artefacts, and frequencies for the network level. The "synchronize" kind of process is not represented explicitly as activities of this kind are continuously materialized through SD and EB meetings.

Table 3: Processes, artefacts, and frequencies for the network level

Governance level	Process	Subprocess	Artefact	Frequency
Drive, continuous improvement, and networking for the governance	perform	drive SPARTA strategy	First principles	yearly
		animate the SD	SD meetings	monthly
		link strategic and high-level objectives	Pilot objectives	yearly
		define leader missions and roles	Leader specifications	yearly
	monitor	ensure efforts are aligned towards high-level objectives	EB meetings	monthly
		ensure high-level objectives are met	SD meetings	monthly
		track contribution of Programs and Activities to high-level objectives	EB meetings (KPI)	quarterly
		ensure leverage factors are exploited	EB & SD meetings	monthly
		measure progress wrt Governance and Management KPI	EB meetings (KPI)	quarterly
		review Governance and Management risks	EB meetings (risks)	quarterly
	improve	improve high-level objectives and KPI	SD meetings	yearly
		improve decision making process from inputs T1.4	Actions from recommendations	yearly
		improve governance (process, rules, bodies) from inputs T1.4 and T2.1	Actions from recommendations	yearly
	liaise	map contributions to European cybersecurity strategy	SD meetings	quarterly
		integrate inputs from other EU and H2020 activities	Roadmap, Skills framework, Pilots focus groups	quarterly

The following artefacts are referred at this level:

- **First principles**: this refers to the SPARTA governing principles[7] as set out in Section 4.1.2 of D1.1 (Bootstrapping a CCN Pilot, PU, M12);
- **SD and EB meetings**: these refer to the (respectively) strategic and operational main bodies as set out (respectively) in Sections 4.1.3.1 and 4.1.3.2 of D1.1 (ibid.);
- **Pilot objectives**: this refers to the pilot objectives as set out in Section 1.1.2 of the SPARTA Description of Action (Annex 1, part B);

[7] For the sake of convenience, we briefly remind those principles here: i. Change the philosophy of risk; ii. Diversity as an asset for innovation; iii. Create opportunities for open leadership; iv. Recognize horizontal leverage points; v. Build digital platforms for forward-looking stakeholder.

- **Leader specifications**: this will constitute a consistent corpus of transversal and scientific and technical specification of the role and expectations put on leaders' shoulders to be built during the third year of SPARTA;
- **KPI**: this refers to the key performance indicators as set out in Section 4.1.4.2 of D1.1 (ibid.);
- **Risks**: this refers to the critical implementation risks as set out in Section 1.3.5 of the SPARTA Description of Action (Annex 1, part A);
- **Actions from recommendations**: this refers to the recommendations stemming from D1.2 (Lessons learned from internally assessing a CCN pilot, PU, M12), D1.4 (Lessons learned from externally assessing a CCN pilot, PU, M27), and the reviews;
- **Roadmap, Skills framework**: these tailor-made artefacts refer to specific instruments which prove to need strong and direct interactions with the ecosystem since the start of SPARTA;
- **Pilots focus groups**: these refers to the inter-pilot focus groups as implemented in parallel to the DG CNECT / 4P meetings and dedicated to specific topical interests.

One specificity of the network-level is that it gathers most of the interaction with third-parties at the exception of a few liaising activities happening at the transversal-level. This ensures that SPARTA's representation keeps high levels of unity and consistency with regards to the strategy defined.

Findings coming from the network-level activity feed the other levels while the other levels also feed the network-level as detailed in the following sections.

3.1.2 Transversal level

Table 4 shows the processes, artefacts, and frequencies for the transversal level. All kinds of process are represented as activities at this level.

Table 4: Processes, artefacts, and frequencies for the transversal level

Governance level	Process	Subprocess	Artefact	Frequency
Adaptation, synchronization, progress measurement, and improvement for governance of community and exploitation activities	perform	propagate strategy to Activities	SD meetings	yearly
		adapt high-level objectives to Activities	SD meetings	yearly
	monitor	perform Activities comparisons	T1.3 meetings	yearly
		measure progress wrt Activities KPI	EB meetings (KPI)	quarterly
		review Activities risks	EB meetings (risks)	quarterly
	improve	improve objectives of Activities	Actions from recommendations	yearly
		improve activities and processes of Activities from inputs T1.4	Actions from recommendations	yearly
	synchronize	ensure interactions between Activities	T1.3 meetings	quarterly
		ensure mutualization of efforts	T1.3 meetings	quarterly
		ensure sharing of practices	T1.3 meetings	quarterly
		ensure transversal consistency between Activities	T1.3 meetings	quarterly
	liaise	ensure interactions with funding mechanisms of Activities	Partnership, Communication & Dissemination	yearly
		ensure fit with business processes	Exploitation	yearly

The following artefacts (not present for previous activities) are referred at this level:

- **T1.3 meetings**: this refers to meetings held in the context of the execution of Task 1.3 (Adaptation, synchronization, progress measurement, and improvement for governance of community and exploitation activities);
- **Partnership, Communication & Dissemination, and Exploitation**: these artefacts refer to specific transversal instruments which require direct liaising activities.

Governance activities set at the transversal level are detailed in Section 3.2 of this document.

3.1.3 Scientific and technical level

Table 5 shows the processes, artefacts, and frequencies for the scientific and technical level. The "liaise" kind of process is not represented as liaising activities from this level are made to flow through the network level to ensure the liaison activities.

Table 5: Processes, artefacts, and frequencies for the scientific and technical level

Governance level	Process	Subprocess	Artefact	Frequency
Adaptation, synchronization, progress measurement, and improvement for governance of R&D&I activities	perform	propagate strategy to Programs and Roadmap	SD meetings	yearly
		adapt high-level objectives to Programs and Roadmap	SD meetings	yearly
		handle change management due to coopetition	T1.2 meetings	quarterly
		facilitate coopeting activities	T1.2 meetings	quarterly
		facilitate posterior use of results	T1.2 meetings	quarterly
	monitor	perform Programs comparisons	Visiting committee	yearly
		measure progress wrt Programs and Roadmap KPI	EB meetings (KPI)	quarterly
		review Programs and Roadmap risks	EB meetings (risks)	quarterly
	improve	improve objectives of Programs and Roadmap	Actions from recommendations	yearly
		improve activities and processes of Programs and Roadmap from inputs T1.4	Actions from recommendations	yearly
	synchronize	ensure mutualization of efforts	Visiting committee	yearly
		ensure sharing of practices	Visiting committee	yearly
		ensure transversal consistency between Programs, and wrt Roadmap	Visiting committee	yearly

The following artefacts (not present for previous activities) are referred at this level:

- **T1.2 meetings**: this refers to meetings held in the context of the execution of Task 1.2 (Adaptation, synchronization, progress measurement, and improvement for governance of R&D&I activities);
- **Visiting committee**: this refers to the Program Visiting Committee as set out in Section 3.3.4 of D1.1 (ibid.).

Governance activities set at the scientific, and technical level are detailed in Section 3.3 of this document.

3.1.4 Assessment level

Table 6 shows the processes, artefacts, and frequencies for the assessment level. The "improve" kind of process is not represented to avoid to introduce meta-concerns about improving the assessments (which are themselves designed to improve the governance). However, it can be noted

it has been planned, for the pilot execution, that the first-year assessment is led internally while the second-year is carried out externally in order to provide different viewpoints and limit potential shortcomings and bias. The “synchronize” kind of process is also not represented at this level as the assessment activity is sufficiently specific not to need extra activities to this aim.

Table 6: Processes, artefacts, and frequencies for the assessment level

Governance level	Process	Subprocess	Artefact	Frequency
Governance assessment and recommendations	perform	prepare the assessment of SPARTA governance	Assessment specification	yearly
		define methods and perimeters to assess	Assessment specification	yearly
		collect data and information from stakeholders	Assessment	yearly
		analyse results along gov, R&D&I, exploit, and comm activities	Assessment	yearly
		make recommendations on expression of objectives	Recommendations	yearly
		make recommendations on process definition and execution	Recommendations	yearly
	monitor	ensure a lightweight assessment process	Assessment specification	yearly
		ensure understanding of partners	Assessment	yearly
		ensure compatibility with operational activities	Assessment	yearly
	liaise	provide feedback to T1.1, T1.2, and T1.3	SD & EB meetings	yearly

The following artefacts (not present for previous activities) are referred at this level:

- **Assessment specification**: this refers to the technical and organizational specification shaping the way assessments are conducted;
- **Assessment**: this refers to the assessment themselves;
- **Recommendations**: this refers to the recommendations coming from the assessment carried out and fed back to the network, transversal, and scientific and technical levels.

Governance activities set at this level are detailed in the series of deliverables D1.2 (ibid.), D1.4 (ibid.), and D1.6 (From assessing to supporting the future CCN, PU, M36) which also detail the results of the assessment activity.

The CCN structure presented above is built from the initial SPARTA governance, described in D1.1 (ibid.), and improved by relying on the second-year operational activities, on feedback provided by D1.2 (ibid.), and on recommendations from the reviewers. As SPARTA is an operational pilot, its governance improvement is iterative; the CCN structure described should be seen as a framework defined at M24 to be implemented during the course of the third year through the SPARTA activities.

3.2 Transversal activities

SPARTA’s transversal activities include the community and exploitation activities. In this section we report on the key governance and management takeaways, with regards to the recommendations that were reported in deliverable *D1.2 Lessons learned from internally assessing a CCN pilot*, as well as to other initiatives that contributed to improving the activities and processes in scope.

As governance and management matured from the project bootstrap year (Year 1) to the intermediate year (Year 2), the focus also turned decisively towards the future CCN setup and

operation. In this vein, it is important to emphasize that the purpose of deliverable D1.2 was to assess the governance of the pilot, not that of the project.

We cluster and reorder D1.2 recommendations that directly concern the community and exploitation activities in Table 7.

Table 7: Recommendations regarding community and exploitation activities (WP8, WP9, WP10, WP11, WP12)

D1.2 reference	WP scope (WP8-WP12)	Description (taken from D1.2)
GC_I1	WP8, WP11	Technical Integration: Clarify the desirable and feasible level of integration between the technical components and results produced by WP4-WP7. Clarify the achievable level of alignment between the four technical programs on the one hand and both WP8 and WP11 on the other.
GC_I4	WP11	Open Source: WP5 and WP6 may need support to engage with the Open Source spectrum in an active and sustainable manner. Could the scope of WP11 be extended by an activity targeting relevant Open Source communities? Are there individuals within the consortium or its group of associates who can and would act as champions?
GC_I6	WP11	Training: The data from the questionnaire and our technical analysis suggest a huge disconnect between WP11 and the technical programs. Is this indeed the case? Is this intentionally so? Would it be possible and desirable to establish trans-WP links?
GC_A4	WP8, WP9, WP10, WP11, WP12	Risk Management: The T1.4 metrics for achieved objectives and the WP13 oriented metrics for the risk of not achieving them is very loosely coupled, if at all. In co-operation with partner INOV, T1.4 could be tasked to investigate whether there are industry-strength methods that offer better granularity, closer coupling, and an integrated view on progress vs. risk. Pilot governance may consider including those objectives that are currently incompletely covered in the list of managed risks. The D1.2 and D2.2 assessments could form the basis of future directory of SPARTA capabilities, supporting governance and stakeholders in building dedicated task forces.
GC_M1	WP8, WP11	Four significant governance aspects are not fully covered yet. They all concern horizontal, co-operative and context-dependent activities: (a) Interaction with external entities and communities for validation and certification; (b) Potential joint activities with European agencies, external research programs and projects; (c) Roadmap updates to reflect new threats and cyber defence technologies; (d) Adjustments and extension of legal analysis to the (yet unknown) actual objectives of an ECCC / ECCN.

D1.2 reference	WP scope (WP8-WP12)	Description (taken from D1.2)
		It should be considered to track these four issues regularly and to include them in the list of risks to be managed.

The D1.2 recommendation concerning the coupling of risks to objectives (see Table 7, "GC_A4") is analysed from the point of view of risk management, by identifying and reviewing risks that are not currently relevant. It is important to note that during the last risk assessment (Periodic Technical Report of October 2020), only 2 risks (out of a total of 28 risks managed for WP8-WP12) were assessed as being currently not relevant.

In the following sub-sections, a report is provided for each of the community and exploitation activities, detailing the pilot governance and execution improvements in Year 2.

3.2.1 Partnership instrument

SPARTA partnership program pulls together people, organizations and infrastructures to strengthen the SPARTA ecosystem. During the first year the main elements (JCCI, Associates/Friends program, SPARTA monthly events, etc.) were bootstrapped while in the second one those have been consolidated.

In particular, the SPARTA program for Associates/Friends was positively launched during the first year in a bottom up fashion. During the second year, efforts have been made by each national cluster of SPARTA countries to consolidate their activities through the increased involvement of other national organizations. Each country followed its own strategy, having however as common guidelines the fact SPARTA wishes to have in its constituency representative of government, industry research and academia, as well as selected grassroots communities.

In terms of community building, in addition to the 44 partners, SPARTA has now added near one hundred among associates and friends. The community also held a plenary meeting in June 2020, despite being delayed due to the pandemic. At the meeting more than 120 participants registered and presented their activities.

The partnership committee has been established and operated to promote and manage the activities of the partnership. Several SPARTA monthly events were performed in many European countries were the SPARTA partners are present and also on request of certain communities, for instance in Switzerland.

This supports the creation of a wider research and innovation community, strongly linked to the SPARTA network. Overall this approach seems coherent with the idea of the commission to set up a community of national active organizations, able to cooperate at European level.

In terms of infrastructures, the SPARTA JCCI Joint Competence Centre Infrastructure, was bootstrapped during the first year with a centralized framework listing the ones jointly available and the virtual education material. In the second year, JCCI has been extended to a fully distributed infrastructure, where organizations can run their local JCCI nodes and advertise the services offered through service description languages (SDL). This allow organizations of the SPARTA ecosystem to offer directly and autonomously services/tools/data that are however centrally represented and indexed. It is worthwhile considering that the effort available in SPARTA only allows to create the infrastructure for hosting the tools, the tools themselves must be provided by other Programs and Activities, as well as by external activities of the SPARTA community.

With respect to GC_I1, the JCCI structure is able to embody the tools developed in the programs. However, it should be noticed that, in the DoA, only the identification and listing of such tools was stated as goal. Thus, the added level of integration provided with the current version of the JCCI is already a step ahead. Several tools are already used by partners and Associates/Friends – for instance for road mapping activities.

With respect to GC_A4 mobilizing 44 partners and several associates is not a simple task. In particular, WP8 did not involve from the very beginning all the SPARTA partners. This made communication and involvement of all the SPARTA partners more difficult. However due to improved communication and re-enforced message about the need of a global involvement, the activities were successfully bootstrapped. The pandemic has been a main issue for an activity as partnership that has on networking and events organization a main ingredient. Some events were delayed and postponed, however in general a good amount of activities has been performed also in the second year.

With respect to GC_M1, the tools of the JCCI and the enlarged community for Associates/Friends are useful both to produce new project proposals as well as for the cooperation for activities as road mapping, as described above. Also, cooperation with organizations as ECSO has been fostered. The cooperation with the 4 Pilots, driven by the Commission has been successful; in particular the last CONVERGENCE event represents a success story of cooperation.

3.2.2 Cybersecurity training and awareness

In 2020, WP9 Cybersecurity awareness and training evolved from the analytical and preparatory phase of year 1 to the working phase of year 2. The results of T9.1 activity focusing on the SPARTA Cybersecurity Skills Framework and T9.2 aiming on mapping of existing cybersecurity courses were used for the delivery of a practical methodology for designing cybersecurity curricula. Furthermore, good-practice curricula were also produced. While the activities of the first year could have been executed rather independently and without intensive collaboration with external partners, the second year's tasks required much more cooperation with other SPARTA work packages and external institutions outside SPARTA.

The internal cooperation with other SPARTA work packages, a requirement mentioned also by recommendations in Table 7, was reflected by further strengthening the communication with relevant SPARTA WPs, in particular with WP6 for the integration of research-related skills to the SPARTA Cybersecurity Skills Framework, with WP8 for the contribution to the SPARTA JCCI common infrastructure involving cyber ranges and with WP12 for external communication, in particular for awareness activities and piloting in outermost regions within the Go Cyber with SPARTA campaign.

The external cooperation, in particular inter-pilot activities, was significantly extended compared to the first year of SPARTA. In particular, WP9 joined two CCN working groups:

- Education Working Group: a group collecting partners from all pilots active in education and training activities. The group is further structured into two strands:
    - Skills Framework Strand: a subgroup focused on the design and implementation of a common CCN skills framework that can be used as a foundation of the European Skills Framework. The group is currently led by SPARTA WP9 partners and meets regularly with CCN members and key institutions, ENISA in particular.
    - Mapping Strand: a subgroup focused on the mapping of existing cybersecurity courses and integration of results of different pilots. The group is currently lead by CONCORDIA and SPARTA is a significant contributor to the university program mapping with its SPARTA Cybersecurity Study Programs map (https://www.sparta.eu/study-programs/).
- Cyber Range Working Group: a group collecting CCN partners active in cyber range technologies. The membership of SPARTA WP9 in this group allowed us to cooperate with CONCORDIA on the deployment and evaluation of the KYPO open-source cyber range.

The CCN inter-pilot activities has been presented at the convergence meeting in December 2020 with SPARTA presenting the results from the Skills Framework strand.

The external cooperation mainly involves ENISA, as its representatives are joining most of the group meetings and are active in WP9 activities. In particular, the datasets from the mapping activities of SPARTA WP9 were presented and delivered to ENISA to be used in the ENISA education map. This

delivery should be the first step to achieve sustainability of SPARTA WP9 results after the project ends. Furthermore, ENISA is active in providing feedback to SPARTA Cybersecurity Skills Framework design and relevant activities. The SPARTA WP9 members are contributing to EU Skills Framework creation through their membership in the ENISA Skills Framework Working Group. In the next period, communication with ENISA will be further extended as concrete tools delivered by SPARTA WP9, such as the Curricula Designer, will be available for comments and evaluation by external organisations.

Although we identified delayed communication as a potential risk in our previous reports, the communication inside and outside SPARTA was relatively smooth during the first and second year, considering the restrictions related to the pandemic situation. However, we expect that the situation may get worse in the next period, as the piloting activities and dissemination require more direct involvement of new partners. While we try to lower the impacts by moving to online space, some activities may be delayed and/or modified. This particularly affect activities involving early adopters in European outermost countries and pilots at professional training intuitions. While these risks are reflected in WP9 management strategy, they cannot be completely mitigated due to unpredictable situation in 2021.

3.2.3 Sustainable exploitation and IPR

Sustainable Exploitation is about making sure that the results of the research programs keep being used and generating value beyond the lifespan of the project. There are two main types of exploitations that are targeted: research and innovation, i.e. the results feed new research and innovation projects, and secondly, commercial exploitation, where the results allow to offer new services or products to the market. This would strengthen the European cybersecurity industry by broadening its offer.

After a first year extremely busy as there were four deliverables expected for the Sustainable Exploitation Work Package, the second year was focused on issues that had been observed.

The most sensitive one was related to what could be called “request fatigue” on the programs’ side. As they were undergoing requests from all the transversal activities, with some overlaps for topics related to privacy for example, it was difficult to get a very engaged response.

This was primarily solved through more interactions at Executive Board and Strategic Direction Board levels, where it was possible to engage directly with the leaders of the concerned work packages.

But in parallel, the WP10 tried to assess if there were some known issues with some of the documents it was requesting from programs. One clear aspect being the lack of perceived value of the documents from the researchers’ perspective, beyond compliance with mandatory requirements of the H2020 framework, such as the existence of a Data Management Plan.

There was also no clear template for building both the document used to assess pre-existing resources, and the report aimed at identifying and documenting the produced results of the research programs. This generated also some friction or lack of engagement. WP10 active participants considered that it may be a lesson to investigate further, even if not directly called for in the definition of the different deliverables. It seemed that a platform could compensate for the administrative overhead as it would facilitate further re-use and increase efficiency through automation.

The point was raised during the first formal review, in February 2020, and led to a fruitful conversation with the reviewers about the suggested solution. Their advice was to start experimenting with a Wiki rather than building a full application.

As the COVID-19 lockdown hit all participants from mid-March to end of May, the operations of the group were slowed down. Nonetheless it finally built a wiki aimed at centralizing data from the Data Management Plan (DMP), the Assessment of Pre-Existing Resources (APER) and Identification and Documentation of Produced Results (IDPR) and limit as much as possible the multiple capture of the same data fields.

The lesson from this first experiment was that both wiki that were used weren't actually solving much as there was still a significant amount of manual work and operations, and automation was limited while the benefit of easy data exchange wasn't demonstrated.

Given the limited time and resources, another prototype was quickly built and evaluated. It consisted in a re-use of the MISP platform and the creation of a new front-end allowing to guide the work of researchers through automated forms, when creating the different types of documents that were requested (DMP, APER, IDPR).

The platform allows not only to manage the different assets needed for the research work, but it also to do it beyond a given project. The owners of these assets can assign them to further projects, without having to enter once more the data related to these assets. The platform allows also to start analyzing various aspects such as Intellectual Property Rights, Privacy issues, or Security of the assets, through specific forms. In terms of governance, this creates an opportunity to prepare the work required for ethics purposes for example, as it can be done through one more form added to the platform.

This should also help clarify the status of the assets with regards to specific risks, such as improper licensing scheme, as these points can be analyzed through the answers to the domain related questions in each form. WP10 intends to use it with this risk reduction goal when supporting the programs in establishing their commercial exploitation strategy, as the platform should allow to spot very easily which assets can generate future problems due to an inconsistent or too restrictive licensing scheme.

We plan to propose to the relevant work packages to experiment with this platform until the end of the project, in order to assess its actual usage value and if it makes sense to invest more in refining its architecture and interfaces. If it were easily adopted, this could become also a very useful tool to be proposed to a broader audience as it could ease the management of research assets for both individual researchers and more institutional teams.

3.2.4 Certification organization and support

In year 2 the certification organization and support have increased cross-cutting collaboration with the CAPE and HAIIT research programs. Initial contacts have been established with T-SHARK and SAFAIR as shown in the figure below.

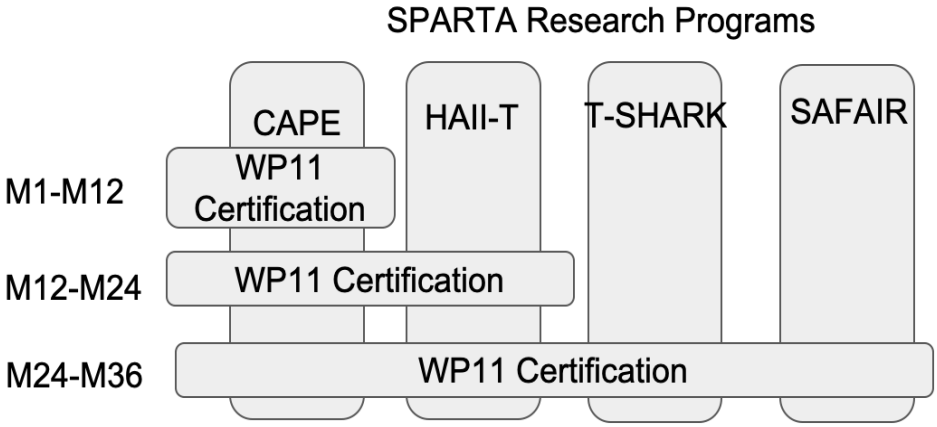

Figure 1: Status of cross-cutting certification activities

The above figure shows the evolution of cross-cutting certification activities with the research programs over the periods M1-M12, M12-24 and M24-M36. Certification activities within WP11 have focused on producing the WP11 deliverables with cross cutting activities in support. The main planned cross-cutting certification activities are with the CAPE research program in which several WP11 partners are involved. This has started at M1 with the topic of efficient certification processes and incremental certification that have been identified as a high priority research topic in T11.1 and T11.3. This has led to aligning the CAPE certification effort towards these goals by attempting to integrate incremental certification processes into cybersecurity assessment processes. The topic of

certification of software development processes, as opposed to product-oriented certification, is the research topic of T11.4 and is being investigated as part of task T5.3 in the CAPE research program. Cross-cutting certification activities with the CAPE are planned until M36.

Following the M12 review recommendations, the certification cross-cutting activities with the other research programs has been initiated. In the period M12-M24 cross-cutting activities with the HAII-T have been started to understand potential links to certification. This has been implemented in the form of regular audio conferences with the individual HAII-T tasks to help them identify and understand some of the certification schemes identified in D11.1 as potentially relevant to SPARTA. It must be noted that WP11 partners are not involved in the HAII-T research program, which make it more difficult to implement the same type of experimental collaboration as with CAPE. However, some experimental activities are the topic of discussions especially in the area of privacy. Cross-cutting certification activities with the HAII-T are planned until M36.

Initial contacts with the T-SHARK and SAFAIR research programs have revealed little need for certification. However, contacts with the two research programs will be continued throughout the M24-M36 period.

Interaction with national cybersecurity authorities involved in SPARTA on the topic of certification is the topic of T11.2. Meetings are planned with the national cybersecurity authorities in the M24-M36 period and one of the topics of discussion will be results from cross-cutting certification activities. Topics of interest that will be discussed with national authorities include need for more efficient certification processes and incremental (product) certification and certification of software development processes.

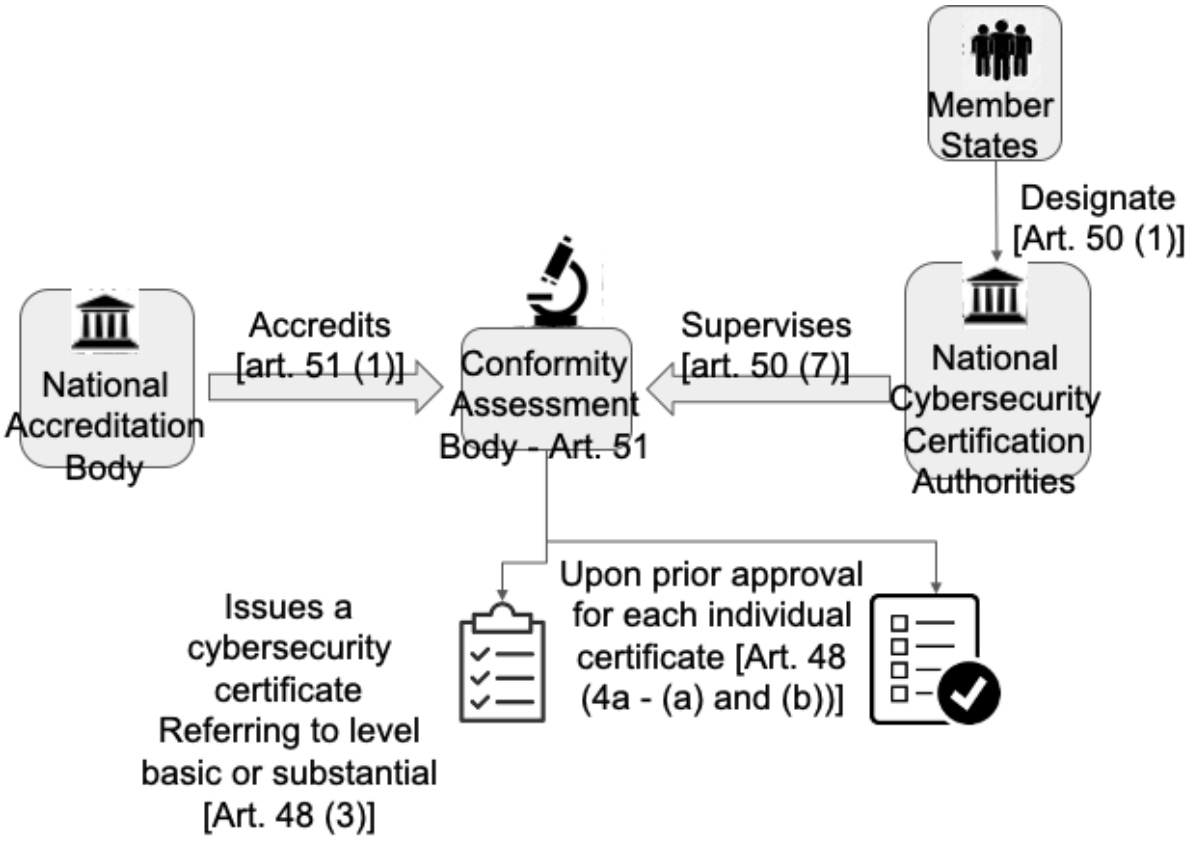

Figure 2: Conformity Assessment Bodies

The above figure shows the conformity assessment bodies as planned in the EU Cyber Act. It can be seen that members states designate national cybersecurity authorities that will supervise the conformity assessment bodies (CAB). CABs are in then accredited by the national accreditation bodies. CABs issue cybersecurity certificates upon prior approval of each certificate by the national cybersecurity authorities.

The Commission and ENISA are responsible for assessing the efficiency and use of adopted Cyber Act certification schemes (Evaluation and review of schemes – article 49-8, from voluntary to mandatory certification – article 56-3). If necessary, the Commission may ask ENISA to start a revision for a given scheme. Useful feedback on the application of certification schemes could certainly be provided by CABs and national cybersecurity certification authorities to the Commission and ENISA.

But beyond providing data directly related to certification schemes CABs could share innovations related to certification via workshops with the national certification authorities. For example, the results of experiments on incremental product certification, or the comparison of process versus product certification could be shared in this manner. Also, a compilation of best practices with respect to certification such as in aviation safety could be shared in a similar manner between CABs and national certification authorities.

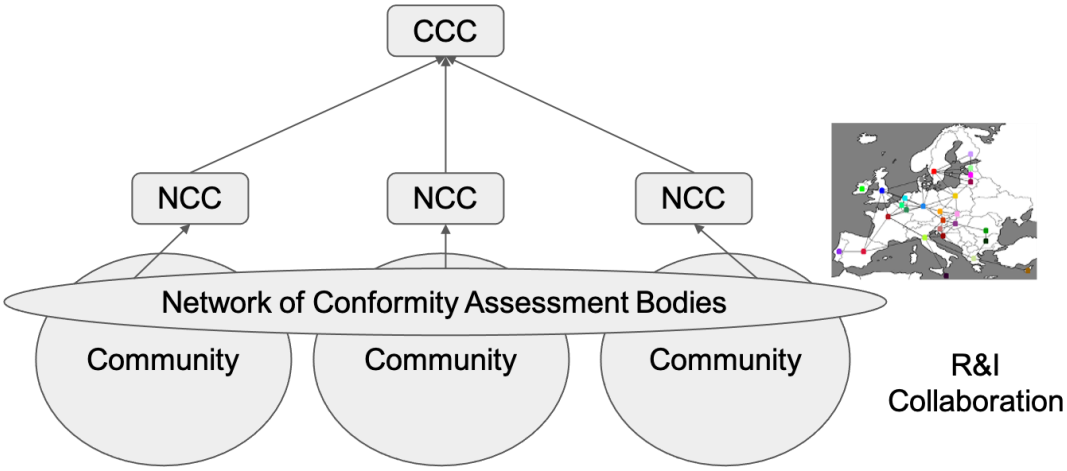

Figure 3: Network of evaluation facilities in the CCCN

Projecting this kind of collaboration between CABs and national certification authorities beyond the SPARTA project could give the following organization described in Figure 3 in the context of the future CCCN. A European network of CABs could be created as a sub-group within the CCCN community to share innovations related to certification. This idea will be detailed in D11.3. Sharing of more confidential data related to certification would be done on a national basis between CABs and their national certifications authorities, before being communicated to the European Commission.

Regarding the recommendations in Table 7:

- GC_I1: Collaboration between WP11 and CAPE is working well, collaboration between WP11 and HAII-T is progressing. And collaboration between WP11 and T-SHARK and SAFAIR is at an initial stage.
- GC_I4: the open-source dimension is not being taken into account in certification.
- GC_I6: this is being addressed by the cross-cutting activities between WP11 and the research programs as reported above.
- GC_M1: most aspect of this requirement have not been analysed.

Finally, regarding the risk "*WP11_1 Cybersecurity certification initiatives evolve during project duration*", the EU CyberAct is being closely monitored by WP11, namely several WP11 partners are participating in ENISA *ad hoc* working groups on new certification schemes.

3.2.5 Dissemination and communication

The deliverable D12.1, submitted in April 2019, established the strategic axis for the design and development of the WP12 Dissemination and Communication activities. The axis established for the first year of the project was "Awareness building" – making the project and its aims to acknowledge –, and is being continuously nourished during the project lifetime.

The axis established for the second year of the project is “Participation” – engaging target groups and enable them to understand SPARTA concepts and results achieved. The novelty of the COVID-19 pandemic caused several impacts on the C&D activities planned for the second year of the project, risking the achievement of the objectives set in deliverable D12.1 and deliverable D12.3 (submitted in January 2020), imposing roadblocks to the steady implementation of the Participation axis.

In the Participation axis, the communication efforts aimed to reach higher levels of audiences´ engagement with the project, such as:

- Attendance in SPARTA events;
- Contacts from media;
- Invitation to speaking at external events;
- Demonstrations of interest.

Activities were re-designed and implemented as we learn how to deal with the pandemic impacts and constraints. It was then possible to achieve communication objectives (mentioned above) and to not compromise the SPARTA expected results.

The use of platforms such as Zoom or GoToMeeting for online meetings and the use of social media networks and other relevant media (Cybersecurity and Digital Privacy Newsletter) have shown to be efficient tools to replace face-to-face meetings, events, and communication materials. The participation axis heavily relied on these tools to reach higher levels of audiences’ engagement with the project.

Some of the conferences, workshops, and talks expected to be organized or attended during the second year of the project were cancelled or re-scheduled due to the constraints imposed by the pandemic. In this context, during the second year of SPARTA, Spartans participated in 32 (conferences/workshops/others), organized 4 conferences and 9 Monthly Workshops, most of them through virtual platforms. Most of these events occurred at the international level and gathered a significant diversity of stakeholders.

The strategy deployed on the D12.3 to maximize partners’ contribution through their direct participation in the production of contents to be shared on social media accounts, website, and other relevant media has shown to be efficient, keeping the audiences updated and informed about several aspects related to the SPARTA project and cybersecurity field. This strategy has contributed to growth in the project’s visibility as it has been able to achieve 1065 followers on Twitter, 422 on LinkedIn, and 195 on Instagram, and create a more consistent and engaged audience.

The SPARTA website was often updated and worked on, in collaborative work between all WPs, led by INOV and CEA, to ensure SPARTA delivers a dynamic, intuitive, and complete platform to its visitors:

- The website provides information about SPARTA, its challenges, structure, and partners on a single page.
- The “Results” page features all the SPARTA publications, deliverables, podcasts, and demonstrators.
- The website has a dedicated section to the training and awareness WP9 and others to the Gender and Diversity dimension of SARTA.
- A “News & Events” section features the frontpage to provide visitors with the latest news, activities, and achievements related to the project.
- The JCCI is part of the SPARTA website and will be leveraged through several publications on social media.

During the second year of the project, SPARTA reached higher levels of (1) attendance on SPARTA (online) events, received (2) contacts from media (e.g., Cybersecurity and Digital Privacy) and several (3) demonstrations of interest through the Friends and Associates programs.

The SPARTA gender and diversity dimension has been enhanced during this period, allowing for more incisive actions and collaborations, namely with the Women in SPARTA campaign.

WP12 is committed to continue building even straighter communication flows with SPARTA partners to ensure that the SPARTA impact is duly communicated to the SPARTA stakeholders. These straighter communication flows will respond to the reported difficulties by WPs related to internal communication as being a roadblock on some tasks. Namely, WP12 is reacting to the current constraints imposed by the pandemic and related risks, searching on how to leverage all the communication through online platforms and on how to strengthen the communication between all partners.

3.3 Scientific and technical activities

SPARTA's scientific and technical activities include the roadmapping, and research program activities. In this section we report on the key governance and management takeaways, with regards to the recommendations that were reported in deliverable *D1.2 Lessons learned from internally assessing a CCN pilot*, as well as to other initiatives that contributed to improving the activities and processes in scope.

As governance and management matured from the project bootstrap year (Year 1) to the intermediate year (Year 2), the focus also turned decisively towards the future CCN setup and operation. In this vein, it is important to emphasize that the purpose of D1.2 was to assess the governance of the pilot, not that of the project.

We cluster and reorder D1.2 recommendations that directly concern the scientific and technical activities in Table 8.

Table 8: Recommendations regarding scientific and technical activities (WP3, WP4, WP5, WP6, WP7)

D1.2 reference	WP scope (WP3-WP7)	Description (taken from D1.2)
GC_G4	WP4, WP5, WP6, WP7	**Cooperations:** Consider co-operation with external initiatives and initiation of independent proposals to extend SPARTA's technological scope. E.g.: calls, projects and initiatives for Secure Society, securing Open Source components, Open Hardware, lowering the barriers to formal verification, changing the "geeky" image of verification into the next cool thing (motto: "programming without verification is something for script kiddies"), etc.
GC_G7	WP4, WP5, WP6, WP7	**Alternate Models / Contingency Planning:** Consider experiments for emulating the structure and operation of National Competence Centres and clusters, and for developing corresponding interaction models. One or multiple of the WPs for the technical programs might serve as a conduit: • The scenarios to be modelled can focus on Lithuania (WP4), Italy resp. Germany (WP5), France (WP6) and Spain (WP7). All work packages, but notably WP5 and WP7, could use some support from ELSA specialists to determine the respective institutional and legal framework.
GC_I1	WP4, WP5, WP6, WP7	**Technical Integration:** Clarify the desirable and feasible level of integration between the technical components and results produced by WP4-WP7. Clarify the achievable level of alignment between the four technical programs on the one hand and both WP8 and WP11 on the other.

D1.2 reference	WP scope (WP3-WP7)	Description (taken from D1.2)
GC_I2	WP4, WP5, WP6, WP7	**ELSA aspects:** The technical work packages WP4 and WP7 actively address areas of potential ethical, social and political concern. They are low hanging fruits for intensifying WP2 (ELSA related activities). Some effort should be invested to determine whether areas of particular ELSA relevance could be located in WP5 and WP6.
GC_I3	WP4, WP5, WP6, WP7	**Synergies:** WP5 develops methods for infrastructure and "systems of systems" analysis. Could the results be beneficial for other technical WPs? E.g., are these methods applicable to analyse parts of the technical setup of WP4 or of task 11.4?
GC_I4	WP4, WP5, WP6, WP7	**Open Source:** WP5 and WP6 may need support to engage with the Open Source spectrum in an active and sustainable manner. Could the scope of WP11 be extended by an activity targeting relevant Open Source communities? Are there individuals within the consortium or its group of associates who can and would act as champions?
GC_M1	WP3	Four significant governance aspects are not fully covered yet. They all concern horizontal, co-operative and context-dependent activities: (a) Interaction with external entities and communities for validation and certification; (b) Potential joint activities with European agencies, external research programs and projects; (c) Roadmap updates to reflect new threats and cyber defence technologies; (d) Adjustments and extension of legal analysis to the (yet unknown) actual objectives of an ECCC / ECCN. It should be considered to track these four issues regularly and to include them in the list of risks to be managed.

In the following sub-sections, a report is provided for each of the roadmap and research program activities, detailing the pilot governance and execution improvements in Year 2.

3.3.1 Roadmap instrument

In year 2, substantial progress was made in implementing governance aspects. Through various SPARTA workshops, but also events and meetings (mostly virtual since March 2020) with associates as well as with other pilots and other communities preparing roadmaps we received a lot of feedback. This enables us to validate and refine the roadmap. There was close coordination with national research roadmap activities, especially in France and Germany, so that topics from the SPARTA roadmap have already found their way into these national roadmaps. The roadmap is revised annually so that it reflects possible new threats and emerging new technologies, such as trustworthy open source hardware.

Adherence to SPARTA's research governance activities evolution

The SPARTA roadmap was presented and discussed in internal SPARTA meetings as well as at two online workshops with external partners. It was also presented in an internal ECSO meeting. In

order to get feedback from a broader community, a questionnaire was developed and put online asking for comments and contributions to sharpen the roadmap.

Roadmap sustainability

The roadmap is regularly being revised and updated based on input from academia, industry and innovation community. Priorities proposed by other international initiatives (e.g., ECSO) have also been taken into account as well as the lessons learned from the rapid digitization due to the Covid19 pandemic.

Roadmap focusing mechanisms

In order to involve a wide range of experts in the roadmapping process, it proved expedient to create synchronous, interactive comment and discussion options (e.g., uni- & multilateral virtual meetings, workshops, etc.) as well as to open up an opportunity to make asynchronous contributions (e.g., online questionnaires). For the latter, it made sense to specify a pattern so that the input can be processed in a structured manner. Thanks to the agile, iterative roadmap development in SPARTA, a roadmap release is created annually. As a result, new findings can be incorporated into the new release within a very short time and dynamic changes can be taken into account promptly. It also seems important to include sustainable topics that are not subject to strong dynamics, such as an open source strategy to increase digital sovereignty, in addition to the technology topics.

Cross pilot coordination

SPARTA is leading cross-pilot coordination efforts that aim at harmonizing the detailed pilot roadmaps into a consolidated guideline with contribution from all pilots towards the common mission of strengthening Europe's digital sovereignty.

3.3.2 Programs

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

Activities within the T-SHARK program are very collaborative and require significant governance efforts by design. The aim here is to build and demonstrate the integrated synergies of several autonomous technological developments (further referred as Sub-cases), providing a backbone of comprehensive cybersecurity.

During the first year of development, focus was put on the identification of value added by individual Sub-cases and the elaboration on potential extensions towards the comprehensive cybersecurity. During the second year, our focus has moved from individual, towards integrated actions.

The cooperation dimension within T-SHARK should be described in two dimensions – internal (enhancing synergies) and external (involving activities beyond the program). Internal cooperation was a very important aspect during the second year, as individual Sub-cases had to demonstrate interconnectivity (in terms of triggers (inputs) and outputs, that are to be used by other Sub-cases) and align the structure of information they were able to share in structured (through Information Sharing Platform) and unstructured (as a Feed) ways in order to combine the full-spectrum awareness scope. This was more of a technical nature, but also required a lot of dialog, explanations and modifications.

The need for external cooperation became significant after the first year of activities. Sub-cases, active within the program, contribute rather fragmented and in that sense limited capabilities to a full scope demonstration of the comprehensive cybersecurity concept. After finalizing the Stage Gates#1 activities, it was decided to try to extend the involved technological solutions by inviting external projects to join Stage Gates process and possibly to be included in the demonstration of capabilities (under the Umbrella case of Elections Interference). Pilot activities were carried with one project (SAPAN). This experience of involvement of external projects provided valuable insights for further involvement activities. It should be noted that external involvement appeared to be more difficult than expected, and required handling a number of issues, like confidentiality, integrity, etc.

While building experience and knowledge during the governance process, that is embedded in T-SHARK activities as a separate Task, there were significant efforts to identify, describe and pilot different aspects of innovation governance. These efforts are more detailed in the next section.

Adherence to SPARTA's research governance activities evolution

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

During the first year the main focus was made on implementation of Stage Gates methodology and application of TRL as a main measure to follow the maturation of innovative developments. The first year ended with several observations:

- The technology-centric orientation of Sub-cases made them difficult to describe.
- We noted a low involvement of end-users and external stakeholders in guidance process.
- Activities were mainly measured by TRL and based on SOTA – and this is not enough.
- Limited considerations on integrity and up-take difficulties observed within technological developments.

Those findings led to search for extensive models of innovation governance, that could describe different aspects of initiatives and help understanding the essence of the value provided, help in identifying integration and synergy aspects, and yield longer term maturation perspectives, including up-take stage.

Main activities during the second year focused on certain aspects of governance:

- Individualized workshops with Sub-case developers. Emphasis was made on fit to concept and link to other sub-cases.
- Set of frameworks were developed, that allows to describe individual developments in comparable and integral manner.
- Started integration of outside SPARTA project into the Stage Gates process.

The main research governance evolution can be summarized in defining and piloting few new frameworks:

- TRL, supported by SRL and MRL - describes maturation and development progress.
- Analytical canvas framework - describes development in standard way allowing to map, cross-integrate and compare.
- Functionalities framework - describes new functions and at what level (strategic, tactical, operational or technical) they are to be applied.
- Analytical techniques framework - describes the methodological core of the innovation.
- Innovation type framework - facilitates reduction of complexity to ease up-take process.

The current state of T-SHARK's research or innovation governance is not at the final point, where final conclusions can be drawn. Piloting, modifying and finetuning activities are still to be planned ahead.

Interaction with transversal activities

Activities in T-SHARK became very relevant to the development of the Skills Framework within WP9. One of the main shortfalls of a majority of frameworks, is their inability to include new, emerging technologies, threats, methodologies or other aspects into their structures. In other words: skills frameworks usually provide descriptions of the past. While validating the Skills Framework within WP9 T9.1 activities, one of the tasks was to evaluate the Adoptability of the framework – referring to the ability to include emerging, new aspects into available structures, or expand them. Frameworks that are able to adapt quickly can provide additional value by signaling, at an early stage, new issues to be considered by all relevant stakeholders. T-SHARK provided a list of aspects that could be included into the Framework. A joint workshop was organized to discuss the possible ways of the inclusion of new items. The workshop provided valuable inputs on framework governance aspects for further consideration.

Friendly coopetition

Stage Gates methodology applied in T-SHARK Program is of the competitive nature by design. Initially they provided a path for competing solutions, that are evaluated at each Gates and some continue their activities, while some drop out and are not further developed. Evaluation is usually based on comparison.

Experience within T-SHARK showed, that this methodology can be used also for the different solutions, that are not competing with each other, nor are directly supplementing each other. Sub-cases in T-SHARK are of a very different nature (some very technological, some are tools to assist human analytics, etc.) and they are at very different development level (TRL). Stage Gates in this context turned to be more facilitating instrument, that enables to provide developers with external feedback. All Sub-cases are developing their solutions in autonomous manners at the beginning. But during the period after SG#1, where the general idea was validated, there is a possibility not only to make another evaluation in SG#2, but also compare the progress achieved. On the other hand, all Sub-cases became linked to each other and focused on generating synergies and joint results. Thus, these Sub-cases become more cooperative while still aiming to get positive evaluation by the Arbitrage Group members.

The overall application of Stage Gates methodology in T-SHARK moved from a competitive nature to more of a co-development mode. Even attempts to understand how they are related and can create joint results are very important in terms of improved individual Sub-case development and in building a comprehensive, well integrated picture, where all Sub-cases play dedicated roles.

Research focusing mechanisms

T-Shark is a highly ambitious and wide scale research program. Research is focused in three dimensions – first of all it defines a new approach for cybersecurity while moving from reactive nature towards predictive nature: in that sense trend analysis as well as the potential development of course of actions is one important aspect. Secondly prediction requires large scale of different factor integration and correlation. Thirdly moving from incidents handling towards threats prediction requires a set of new methods and overall approaches. All of this results in a highly differentiated innovation effort that is governed using program and projects portfolio principles, defining entry/exist criteria for the evolution of each individual technical development supported by constant end-user advisory board validation. Each technical team is left with a wide autonomy on the organization of implementation activities.

Having a final integrated method is the core goal of common efforts. To ensure this, the program periodically runs integration workshops and has agreed on “umbrella integrated scenarios” to be supported by all technical implementations in order to aim for an end-to-end solution.

At the same time, the nature of the problem addressed in T-Shark demands for cross-border operational execution, therefore cross-alignment between different MS regulatory frameworks and technical cybersecurity standards are used. This is yet another important aspect to be followed.

All of that results in an integrated international research organization combining technical, societal, legal and methodological innovations into one solution.

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

Time horizon

Individual T-Shark technical innovations are focused on concrete challenges identified in current cybersecurity operational environments and will be made available immediately after the complete program implementation.

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

T-Shark has contributed to the “Moonshots” initiative and has defined future developments perspective for another 7-10 year for complete challenge realization.

Societal and ethical perspectives

The T-Shark research program has addressed societal, legal and ethical perspectives in its design, with a separate activity being dedicated to the abovementioned aspects. During Year1 more than 20 separate challenges have been identified and grouped in 3 mega challenges, those have been researched during Year2 of the program implementation. Currently performed research and in-depth analysis include information gathered from 18 MS. In parallel, a legal assessment per each individual technical subcase development has been conducted, serving as major input to the integrated techno-societal innovation development plan for Year3.

To validate analysis results and hypotheses, 2 legal moot-court exercises have been conducted during Year2 and one EU level Moot Court exercise has been planned in cooperation with an EU Legal Moot Court event during 2021.

T-Shark continuously interacts with WP2 to facilitate transversal SPARTA activities and provide program-related contributions to general developments.

At the same time contributions to the ELSA analyses are provided. Research Program assessments have shown that it has well balanced execution in terms of all major ELSA aspects.

During each Stage Gate event, technical subcases intermediary results are assessed not only using TRL but also different SRL criteria that provide comprehensive views on innovation development.

Enabling partnerships in research governance

Involvement of project external stakeholders into the overall project governance is usually rather challenging, and mostly limited to involvement in different project management bodies. When it comes to the more specific activities within the project, involvement becomes even more difficult, as no short-term benefits are foreseen.

The main instrument enabling partnership in the T-SHARK research governance, is the Arbitrage Group (AG). The AG consist of experts from different fields. There are representatives of industry, academia, end-user organizations, policy makers and project internal experts. The role of the AG is to evaluate Sub-cases during SG events. But evaluation is perhaps less important than feedback and questions, which provide the most value for Sub-cases. Currently over 15 different experts are involved in the AG activities. Even though they meet once a year, they have a possibility to get deeply involved in understanding the individual developments and the concept of comprehensive cybersecurity as a whole. Two additional instruments are the set of criteria and the umbrella case, providing structure for their involvement. Each group of experts are provided with the list of criteria before the SG event. There are individual sets for each group, so that policy makers are not asked to provide feedback on technology-specific aspects or industry representatives are not asked about the fit for EU priorities or specific ELSA issues. The umbrella case provides a narrowed context of evaluation and allows to move from very generic, high level, evaluations to more specific, understandable contexts.

Even though activities around AG within T-SHARK are of a piloting nature, it already appears that this approach of enabling partnership is valuable. Specific benefits for AG members are proposed, but there must be more efforts allocated to develop and keep the AG as a community. It would also be useful to discuss possibilities to construct an AG type of body, able to get involved in different EU projects research governance.

Governing research outputs

During Year 2 of the T-SHARK implementation, the Program Portfolio Management approach has shown its potential: we were able to demonstrate 2 technical subcases progress maturation leading

towards market-ready services, those have been introduced correspondingly in Poland and the Czech Republic, further technical solutions are foreseen for Year 3.

The Arbitrage Group instrument has also contributed to the orientation of R&I&D activities by giving early-stage end-users insights and prioritization leading towards better market readiness.

The Umbrella Demo Case (Elections Interference) gave an opportunity to all stakeholders groups to unlock future integrated solution potentials by giving the integrated perspective and was well welcomed by practitioners.

At this time, several key points appear in T-SHARK:

- Having an “Umbrella Demo Case” defined for several technical and societal innovations governed under one common research program has allowed to integrated the work of different maturity level R&D initiatives also combining technical and societal aspects of the problems, gaps and challenges identified.
    - Recommendation for future CCN: define a few end-user story lines to illustrate different aspects of each mega challenge, thus providing mission-oriented seamless activities governance and coordination
- The Arbitrage Group representing 5 user categories (practitioners, academia, industry, policy, technology) has shown its potential for very comprehensive – almost 360 degree – validation of the program’s progress. This feedback loop has been highly welcomed by the T-SHARK research program members.
    - Recommendation for future CCN: introduce multi-disciplinary innovations validation board to maximize innovation readiness in all major aspects (not only technical or functional).
- A common development environment/ecosystem is highly crucial for integrated international research programs, especially involving actors of different stakeholders’ domains (national security, public security, industry, research, academia, individual experts).
    - Recommendation for future CCN: consider and provide a development, testing and validation ecosystem for future international integrated R&I&D initiatives where relevant introduce best practices from DevOps as well CD&CI.

3.3.2.2 Program 2: CAPE – Continuous assessment in polymorphous environments

Adherence to SPARTA's research governance activities evolution

CAPE has matured in a very flexible governance model. Technical activities are carried out in the tasks, where tools are discussed in T5.1, vertical 1 and security-safety in T5.2, vertical 2 and open-source in T5.3, contribution to certification in T5.4 (started only recently). As a result, teleconferences are organized every two weeks at task level and monthly at program-level. This provides a very flexible yet redundant governance model, which naturally maximizes interactions within the program.

All task leaders and WP leaders are experts in the field, and easily delegate presentations to program contributors. This lightweight governance also works because of the quality of the contributions from the program participants.

Interaction with transversal activities

Policy activities related to certification are naturally handled with CAPE, as partners involved in WP11 are also present and active in CAPE.

Friendly coopetition

The CAPE program chose to demonstrates a cooperative mode of management. Several tools have the same (or very close) assessment targets. Rather than implement twice times the same tool (with different techniques), we harmonized the specification of the tools so that they had complementary goals. This deliberately implemented a cooperating rather than a competing governance model, focusing on leveraging synergies and competencies between researchers to extend the coverage of our research activities. The joint design and sharing of the two verticals are also representative of the governance of CAPE, where people, competencies and platforms are collaboratively shared to elaborate advanced research platforms.

Research focusing mechanisms

CAPE offers a concrete materialization of cybersecurity and safety assessment and validation in two concrete examples. This prepares the upcoming second cycle of design-implement-validate for the tools in CAPE, as well as the work on certification profiles and cybersecurity certification started earlier in CAPE, in association with WP11.

In terms of governance, deliverables D5.2 and D5.3 provide an example of how CAPE partners have successfully been able to collaborate towards an integrated research and validation workflow. This is particularly important as evaluation and validation is the conclusion and an extremely important part of research. It often is extremely expensive for individual researchers. The mutual exchange and joint elaboration of validation tools and processes is thus an important lesson-learnt from CAPE.

In a nutshell, the major research-focusing mechanism in CAPE has been the development of use cases accessible to all project participants, with a sufficiently broad scope and sufficiently easy access that anyone could easily participate.

Time horizon

There are two extremely different time horizons in CAPE.

On one hand, what is done related to use case 2 (“Complex System Assessment including large software and open-source environments, targeting e-Government services”) is extremely close to being usable immediately, by anyone, and has already been opened and made available to a wide community. In a nutshell, part of the CAPE production is already on the market, or very close to being released.

On the other hand, what is done in CAPE related to use case 1 (“Connected and Cooperative Car Cybersecurity”) will only bear fruits much later than the end of the program, for multiple reasons. First, the compromise between security and safety is difficult to establish, and we are barely scratching the surface of what that means, and starting to formulate the initial theoretical models. Second, what is studied in CAPE, the platooning scenario, is very limited. We are, for example, not taking into account cars joining and leaving the platoon. Third, there is a significant effort to bring that, even from an experimental perspective, out of the lab and towards first real life experiments. This in fact is quite exemplary of the difficulties of applying cybersecurity in the context of cyber-physical systems.

Societal and ethical perspectives

CAPE contributes to the general objective of cybersecurity, increase trust in digital services and promote usage and development. The link with ELSA occurs through involvement of partners in certification development activities (experts contribution to ENISA working groups on the topic), and as such is addressing the legal and regulatory framework.

Another ELSA aspect of CAPE is insurance, for both use cases, to enable tracing responsibilities and failures in systems. For the Connected Car use case, CAPE needs to take into account the insurance aspects related to accidents in case of failure, and the ability to understand where in the cyber-physical system the failure occurred (e.g. which car, which subsystem in the car, etc.). For the Complex Software System use case, CAPE needs to consider the management of new risks, i.e. dealing with vulnerabilities that are discovered in parallel to deployed and operational systems (e.g. vulnerability impact, patch strategy, etc.)

Enabling partnerships in research governance

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

Governing research outputs

As mentioned previously, several outputs are already available as open source.

The other outputs should be considered contributions to long term research.

Another, more difficult to elaborate, output is our use case platforms. We will study plans for preservation of these platforms beyond the project.

At this time, several key points appear in CAPE:

- Understanding where one's research (and others) is positioned is important for fruitful dialogue and integration. In CAPE, this takes the form of the extended V-cycle defined in D5.1. This means that researchers understand what the SoA is and what expectations they have in terms of inputs to their research, and what kind of expectations others have on their research outputs.
    - Recommendation for future CCN: define using a common taxonomy the problem addressed by the tool, its requirements, interfaces and outputs.
- Redundancy in interactions is essential. CAPE maintains five interleaved interaction paths (WP and tasks), with regular interactions planned independently of one another. As a result, there are over 15 monthly teleconferences and meetings in CAPE, enabling strong and continuous engagement of participants without imposing undesirable constraints on their schedules. Interactions are recorded with plaintext minutes, to enable easy catch-up. Absence of one of these paths for a few weeks has little impact on the project as a whole.
    - Recommendation for future CCN: encourage shared responsibility for research and redundancy in research paths and activities.
- Focus on use cases helps interactions, common understanding, and problem solving. The needs of a use case, the data formats and interfaces, the vulnerabilities and attacks that can be deployed, create a common understanding and goal. It creates also the additional difficulty that some tools may not fit the use case. In CAPE, this was dealt with by either selecting only one of the two use cases (the major strategy) or seeking the appropriate content in one of the use cases through a small extension (the minor strategy). The combination of both strategies has successfully enabled all contributions to be deployed in CAPE.
    - Recommendation for future CCN: share use case requirements, interfaces, and possibly datasets, to foster an active research ecosystem (through a JCCI-based platform for instance).

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

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

Since the beginning of our operations in Year 1, we immediately understood the importance of defining a single, shared environment for staging our demonstrations and for driving the integration process. Hence, in year one we started developing a unified case study where each partner contributes with a dedicated application scenario. The unified use case is now an asset for fostering both internal and external interactions.

Although central, the use case is not the only interaction activity of HAII-T. More detail on the individual initiatives is provided below.

Adherence to SPARTA's research governance activities evolution

During the first year, we defined the reference model for the security-by-design framework to be used for the implementation of the HAII-T. In Year 2, we further developed this concept and we implemented the first version of the HAII-T demonstrator. The demonstrator implementation included a number strategic activities, e.g., related to privacy-by-design and secure operating systems. All of these activities deal with the practical feasibility of the abstract notion of security-by-design and they required a continuous interaction among the expert partners. In terms of governance, every partner was asked to present a specific application scenario that was both (i) adequate to demonstrate their contribution and (ii) well integrated with the unified use case. This approach allowed every partner to share in its own expertise and to collect feedback.

Interaction with transversal activities

The activities carried out in HAII-T included direct interactions with other work packages and tasks of SPARTA. In particular, during Year 2 we devoted a considerable effort to investigate the relationship between WP6 activities and certification aspects (WP11). Although such an interaction involved all HAII-T tasks, the activity is particularly relevant for T6.5 where GDPR compliance analysis methodologies are investigated. For this and other reasons, we proposed an amendment to extend T6.5 activities, originally planned to terminate at year 2, by an additional year.

Another significant interaction has been recently carried out with the EU pilot project CONCORDIA. One of the goals of CONCORDIA is to study and develop Cyber Ranges, i.e., training environment for cybersecurity education. The activities of WP6 include the creation of virtual replicas of real-world facilities (Task 6.3). We have been invited by CONCORDIA to present our work as a possible enabling technology for the creation of modern Cyber Ranges. Next steps include involving Training activities (WP9) in order to extend this collaboration to the other pilots involved in the CCN.

Finally, the Year 2 demonstrator and the associated virtual environment have been proposed as WP6 contributions to the SPARTA JCCI platforms. This contribution will be finalized during Year 3.

Friendly coopetition

Joint publications derived from the collaboration in WP6 have been already presented in Year 1. This also continued during Year 2. In particular, all the partners agreed on submitting a joint paper describing the HAII-T application scenarios (in preparation).

Moreover, during year 2, DIOT srl joined the SPARTA Friends program. DIOT srl is an Italian, innovative startup developing IoT devices for smart home environments. The overall goal is to apply the SPARTA HAII-T technology for the security assessment of DIOT products.

Research focusing mechanisms

WP6 activities focus on intelligent infrastructures. These infrastructures can have different sizes and belong to different kinds of organization, from small, e.g., smart homes, to large scale, e.g., critical infrastructures and smart industries. In Year 2, we agreed on developing a unified use case that includes several aspects that are common to most intelligent infrastructures. The unified use case is driving the integration process and proved to be a strategic asset for the entire WP and for SPARTA in general.

Time horizon

HAII-T deals with existing problems in the security of smart environments. The unified use case has been designed by including technologies and components for the real world. We expect that the activities carried out in the virtual environment can be readily ported to the real infrastructures.

Societal and ethical perspectives

During Year 2, WP6 started a regular interaction with the ELSA programme. In particular, we carried out dedicated meetings and discussions for identifying the ELSA-related topics in WP6. Among them, privacy issues received major attention (see above). The activity is still ongoing and it will be finalized in Year 3.

Enabling partnerships in research governance

The Year 2 demonstrator relies on two strategic assets, i.e., the virtual infrastructure and the application scenarios contributing to the unified use case. These represent a valuable resource that we are planning to release to the community. The public presentation of these assets will occur through publications, deliverables and code repositories. Our goal is to provide the community with case studies for testing and training.

Governing research outputs

HAII-T is meant to provide a contribution to the community of smart infrastructures designers and developers. In particular, demonstrators should raise the bar of security assessment for the intelligent infrastructures.

Both public and private stakeholders are pushing for the development of production frameworks ensuring privacy and security by design. Several efforts are also devoted to the definition of guidelines and best practices as well as tools to foster their verification and application (e.g., see https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool). HAII-T has a strong potential to support the security evaluation and certification of intelligent infrastructures. Year 3 activities will further explore this opportunity.

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

Adherence to SPARTA's research governance activities evolution

SAFAIR participates in the balancing strategic goals and adaptation to changes approach to program governance perpetuated in SPARTA. The SAFAIR program encompasses 7 partners, a small team focused on achieving the program technological and ethical goals. The program delegates representatives to the Executive Board, the body supervising the execution of the SPARTA mission. SAFAIR also contributed to the SPARTA Roadmap, Joint Competence Centre Infrastructure (JCCI) and ELSA aspects. SAFAIR maintains the SPARTA open leadership to foster scientific excellence. SAFAIR, at its core, builds digital platforms that seek to pre-emptively answer the needs of the market, anticipating the immense impact AI technologies will have in the near future, and dealing with some of the still unanswered questions regarding AI – its security, explainability and fairness.

Interaction with transversal activities

SAFAIR took an active role in the contribution to the development of SPARTA Roadmap. Moreover, the leader of WP3 – TUM – is one of the partners on the SAFAIR team. Similarly, SAFAIR contributes to WP2 – ELSA, while at the same time UNamur, who leads WP2 is part of the SAFAIR team. VICOM, who leads the work on JCCI is also on the SAFAIR team and has access to the artifacts produced by the program. Recently, in order to mainstream ELSA-relevant topics SAFAIR published a text on ethical dilemmas in cybersecurity authored by ITTI[8].

On the other hand, SAFAIR is not (and does not plan to be) involved in any certification or standardization activities, rather focusing on quick progress, publications and demos.

Friendly coopetition

SAFAIR organizes a competition (task lead by TUM) as external validation of the results of research conducted. The details of the competition are delineated in D7.3.

Research focusing mechanisms

SAFAIR is the smallest of the SPARTA programs, which allows to perpetuate certain governance concepts not available for larger structures. SAFAIR uses open and lean governance structure without any heavy-like management structures or procedures. The participatory leadership approach creates an environment conductive to research innovation. This is crucial because of the technology-focused nature of SAFAIR and allows to play to the strengths of the partners involved in SAFAIR, acquiring significant synergies. The results of those synergies are clearly visible when consulting the technology-focused deliverables: D7.1, D7.2 and D7.4.

Time horizon

SAFAIR is fully aware of the usefulness and prominence of cross-domain leverage, especially in subjects as ubiquitous as artificial intelligence. To boost the impact of research conducted in SAFAIR, the findings are adapted across different verticals, like cybersecurity or medical imaging. The work conducted in SAFAIR sits at the very forefront of scientific research, dealing with both some of the most pressing, and some of the newest, most current, emerging issues in AI. The horizontal nature of innovation in AI in general and in SAFAIR in particular, ensures that the artifacts produced maintain high relevance across different fields. The digital character of produced results provides quicker and easier adaptability, thus maximizing the impact of the investment.

[8] Available here: https://sparta.eu/news/2020-12-10-ethical-dilemmas-related-to-cybersecurity.html

Societal and ethical perspectives

All data-related technologies are directly linked to ethical and societal aspects. SAFAIR holds a proverbial finger on the pulse of the current legislative environment w.r.t. data protection and privacy protection. At the same time, one of the aspects of the SAFAIR program – fairness of AI – has strong roots in ELSA. One could say, that SAFAIR is the technological twin/arm of ELSA – focused on developing technologies to meet ELSA needs. The consequences of ethical aspects of the proliferation of AI are recognized in SAFAIR and a specific task on developing the fairness ensuring mechanisms is dedicated to that aspect in the program. By the same token SAFAIR remains in communication with the SPARTA-level ELSA work package (WP2). Recently, in order to mainstream ELSA-relevant topics SAFAIR published a text on ethical dilemmas in cybersecurity authored by ITTI, available here: https://sparta.eu/news/2020-12-10-ethical-dilemmas-related-to-cybersecurity.html

Enabling partnerships in research governance

SAFAIR is a small-scale focused research programme. We mainly engage with scientific community at high-quality events such as scientific conferences in cybersecurity or AI (such as CORE-ranked ICCs, IJCNN and ARES) etc.

Governing research outputs

The adoption of the results of SAFAIR research follows a similar pattern of the adoption of AI technologies, as SAFAIR is closely tied-in with those. Wherever AI is used in critical applications the need for security, explainability and, in many cases, fairness arises. Thus, components of the artifacts created in the SAFAIR program can relatively easily find their way to being adopted across multiple different verticals, and products, services and processes related to those.

Chapter 4 Summary and Conclusion

At the end of Year 2, the SPARTA Network of Competence Center pilot has performed significant improvements throughout its Governance Activities, ranging from incremental adaptations to transformative modifications. The work performed on modularizing the approach to Governance, initially suggested by reviewers at M12, has shown to be a success both in improving theoretical legibility, and in driving concrete activities.

There is perhaps no better tribute to the Governance Activities and the Spartans that implemented it, than the fact that it weathered the 2020 COVID pandemic. In the face of generalized confinements, uncertain futures, and rapidly-changing conditions, the SPARTA pilot not only continued to operate successfully, but also produced a remarkable amount of results, despite difficult interaction conditions.

Taking a step back, and looking at the bigger picture, it seems the SPARTA community has strongly evolved with regards to governance. While the first year of the pilot was very much focused on bootstrapping, setting up habits and finding the right interfaces, this past second year has seen SPARTA leaders take ownership for their perimeters, and make governance their own. We know how much effort this has required from them, especially in the current period, and want to recognize their commitment.

Looking to the future, and toward the ECCC, the lessons learned during this work period suggest paying attention to three specific aspects in particular. The SPARTA Associates program should be encouraged to evolve towards a European cybersecurity community. Parallel international activities like the OpenSSF and the OCA could be accounted for. Technical and non-technical activities should be re-evaluated and transitioned to the ECCC, into follow-up activities, perhaps through inter-pilot activities.

Chapter 5 List of Abbreviations

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