SPARTA

D1.2

Lessons learned from internally assessing 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 / D1.2/ V1.0
Work package contributing to the deliverable	WP1
Due date	January 2020 – M12
Actual submission date	10th February, 2020

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

Abstract	This document describes the structures, processes and activities that characterize the governance of the SPARTA pilot during its first year. We analyse these constituents in view of their adequacy for future, institutionalized instances of European Cybersecurity Competence Networks (CCNs) and a European Cybersecurity Competence Centre (ECCC). The analysis concludes with a number of suggestions for adapting PARTA's current governance model.
Keywords	Governance, pilot, structure, process, Cybersecurity Competence Network, Cybersecurity Competence Centre, CCN, ECCC, NCC

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

Editor

Dirk Kuhlmann (Fraunhofer)

Contributors

Florent Kirchner, Augustin Lemesle, Thibaud Antignac (CEA)

Daniel Bachlechner, Susanne Bührer-Topçu, Frank Ebbers, Michael Friedewald, Ralf Lindner, Elisa Wallwaey (Fraunhofer)

Goncalo Cadete (INOV)

Reviewers

Manon Knockaert (UNamur)

Volkmar Lotz (SAP)

Disclaimer

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

Executive Summary

SPARTA is one of four pilot initiatives investigating operative aspects of a future European Competence Centre for Cybersecurity (ECCC). As of January 2020, the precise role, structure, function and topical scope of this institution is still in flux. The adequacy of SPARTA's governance model for a future ECCC is therefore evaluated against a moving target, making this effort a tentative exercise at best.

The primary governance objective of SPARTA for the first 12 months was to ensure the efficiency of project management at the intermediate level of boards and work packages. This required the implementation of a management and reporting framework capable of covering all main activities. The second major objective was to drive and to ensure that its technical and non-technical activities as well as its cyber security research roadmap were streamlined to shifts in the research-political context and the nascent agendas of the three other pilot initiatives.

The first working phase of SPARTA focused on the preparatory groundwork. During this phase of SPARTA, the Executive Board primarily dealt with EC-project management aspects, while the Strategy Direction Board primarily addressed CCN pilot-specific aspects. There was strong utilization of the Roadmap committee, while other governance bodies (notably the Certification Task Force, the Ethics Board, and the Advisory Committee) were under-utilized. This has to be attributed to the early stage of the research programs, the initiatives around certification and training, and to the long lead-up time for baseline studies on legal and ethical requirements.

Given the size and complexity of the pilot, it is not possible to micro-manage its diverse activities at task level. SPARTA's success as a CCN pilot relies on the initiative of the leaders for the technical programs, the work packages and tasks. The program leaders were given substantial leeway to tailor and establish structures and processes that suit their work packages. In view of the growing importance of the technical programs for supporting horizontal activities, interventions from central pilot governance are likely to intensify in future.

From an internal assessment perspective, the efforts to establish the organizational framework for governance have been successful. A pilot-oriented perspective suggests revisiting a number of processes and tracking those horizontal activities more closely that have not fully been covered during the first working period.

At this stage, it is not possible to assess the overall adequacy of SPARTA's governance model as a blueprint for -- yet to be defined -- organizational details of a European CCN or an ECCC. This problem will be addressed again during year two in a follow-up study that takes a pilot external perspective.

For the upcoming period, a number of considerations for governance have been put forward in chapter 6. They concern alternate organizational models, contingency planning, horizontal integration, and the prerequisites for more regular assessments and tracking.

Table of Content

Chapter 1 Introduction 1
Chapter 2 Terminology, Scope, Approach, Methods 3
2.1 Terminology 3
2.2 Scope 3
2.3 Approach and Methods 4
Chapter 3 Research-Political Context 7
3.1 National Competence Centres 8
3.2 Focus and Scope of the Pilot 9
3.3 European Security Certification Scheme 9
3.4 Ethics and Socially Responsible Research and Innovation 10
Chapter 4 Characteristics of SPARTA Governance 12
4.1 The SPARTA Governance Structure 12
4.2 SPARTA Pilot and Project Governance in Practice 13
4.2.1 SPARTA as EC Project 13
4.2.2 SPARTA as CCN Pilot 14
4.2.3 SPARTA Governance in Year 1: Comparing Plan and Implementation 16
Chapter 5 Pilot Governance Assessment 17
Part 1. Pilot-internal Parameters 17
Part 2: General Objectives of SU ICT-03-2018 20
Part 3: Tasks of SU-ICT-03-2018 24
Part 4: Milestones and KPIs 31
Part 5: Potentials of the Technical Programs 35
Part 6: Views from the Trenches 38
Part 7: Assessment Assessed 40
Chapter 6 Recommendations, Lessons Learned, Outlook 44
6.1 Considerations for Pilot Governance 45
6.2 Lessons Learned 48
Chapter 7 Summary and Conclusion 49
Chapter 8 List of Abbreviations 50
Chapter 9 Bibliography 51
Annex 1: Governance Assessment Questionnaire 2019 52
Annex 2: Assessment aspects, KPIs and Milestones 58

Annex 3: Assessment Aspects and Managed Risks 61
Annex 4: Statements from European Institutions 67
Annex 5 List of Partners..... 71
Annex 6 Cheat Sheets for Technical WPs 4-7 73

List of Figures

Figure 1: Assessment Workflow -- Table: Assessment Single Tasks 6
Figure 2: Organizational structure 13

List of Tables

Table 1: Cross-Task Involvement 18
Table 2: Perceived Dependency 19
Table 3: SPARTA's coverage of governance aspects (estimate for Dec. 2019) 21
Table 4: Colour coding of assessment aspects 24
Table 5: List of all tasks from SU-ICT-03-2018 25
Table 6: List of generic Governance Tasks 26
Table 7: List of Technology related Governance Tasks 27
Table 8: List of Network related Governance Tasks 28
Table 9: List of Demonstrator related Governance Tasks 29
Table 10: Decomposition of demonstrator-related aspects 29
Table 11: List of Assessment related Governance Tasks 30
Table 12: Aspects for regular monitoring via assessment (A) and KPI (X) 32
Table 13: Possible ECCC Objectives 35
Table 14: National / geographic Distribution of WP4 Partners 36
Table 15: National / geographical Distribution of WP6 Partners 36
Table 16: National / geographical Distribution of WP6 Partners 36
Table 17: National / geographical Distribution of WP6 Partners 36
Table 18: Potentials of Technical WPs 37
Table 19: Estimated Effort for D1.2 Assessment 41
Table 20: Considerations for Governance 47
Table 21: SPARTA Questionnaire Dataset 1 57
Table 22: List of Milestones and Verification Criteria 58
Table 23: SPARTA KPIs up to month12 (taken from DoA Part A,p6) 58
Table 24: Aspects for single assessment 59
Table 25: KPIs not corresponding to any static assessment aspect. 60
Table 26: Relevant managed Risks for Pilot Governance (excerpt SARTA DoA Part A 1.3.5) 62
Table 27: Assessment aspects matched against risks 63
Table 28: Project Governance Aspects and corresponding Risks 65
Table 29: Pilot Governance Aspects sorted by Cumulative Weighted Risk 66

Chapter 1 Introduction

The official mission statement for creating an advanced European institution for Cybersecurity can be found in the "State of the Union" address by then-president of the EC, Jean-Claude Juncker from September 13, 2017. In this speech, he announced the implementation of a set of new tools to improve cybersecurity in Europe, including a new Cybersecurity Agency tasked with helping to defend against cyber-attacks [1].

The September 2019 press release by the EC describes the anticipated tasks of this agency: the development and roll out of tools and technology for state-of-the-art cyber defence and complementary efforts for capacity building in this area at EU and national level. The press release even suggests that this new centre could be further developed in pursuit of a genuine cyber defence dimension [2]. This option aims beyond the tasks currently covered by the European Network and Information Security Agency (ENISA), which acts primarily in an advisory and coordinating capacity.

The aim of establishing a new European Cybersecurity Research and Competence Centre has since been re-emphasized by EC president-elect von der Leyen [3] and was translated by the EC into a pilot research initiative for Cybersecurity Competence Networks with Competence Centres to develop and implement a common Cybersecurity Research & Innovation Roadmap [4]. SPARTA is one of four EC funded projects investigating core aspects of Cybersecurity Competence Networks (CCNs) on a Trans-European scale [5]. Specifically, this investigation concerns alternatives for the functional, procedural, operational and technological characteristics of a future layout for the Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre.

The original call [4] demands the coverage of a sufficiently large subset of the EC's CPPP Strategic Research and Innovation Agenda and an extended at least 9 participating countries. Consequently, the SPARTA consortium is rather large. The number of partners (44) exceeds by far that of a normal Research and Innovation action. Nevertheless, the overhead for operational and technical governance has to be kept roughly within the limits typical for EC funded research. This poses formidable challenges for steering the project. Given the allocated resources, attempts to manage the pilot activities at fine granularity (task level) would quickly overwhelm the project lead acting as the competence hub. Therefore, pilot and project steering have to rely on delegating core responsibilities to WP and task leaders more than usual. The rules for resourcing managerial overhead imposed by the EC funding rules further constrain the options for experiments with governance structures and processes.

In support of assessing the governance of the SPARTA pilot, WP1 includes the dedicated task T1.4 for monitoring the related activities on a continuous or at least regular basis. This regards the activities of the various boards, physical meetings and coordination efforts. The corresponding data traces were retrieved from the project's technical infrastructure (mailing lists, document repositories, project communication server). Additional data points have been gathered via interviews and questionnaires. The first purpose of T1.4, documented in this study, is to gauge the pulse of the project by determining the level of interaction and collaboration between tasks and WPs. The second main objective is to estimate whether the various governance activities, processes and structures are suitable to serve as a blueprint for an institutionalized instance of a cyber-competence network with a coordinating hub at its centre.

This deliverable (D1.2) is the first in a set of three, with D1.4 and D1.6 scheduled at annual intervals. D1.2 covers the first 10 months of the project[1]. During this period, WPs and tasks needed time to ramp-up their activities, to "find their feet" and to initiate kick-off activities in support of getting the project as a whole off the ground. Hence, we are assessing a work period mainly characterized by establishing feasible processes and structures for cooperating at task, work package and project

[1] Editing cut-off for D1.2 in January 2020

level. The first assessment in D1.2 is therefore dominated by an internal perspective. In accordance with SPARTA's *Description of Actions* (DoA) [16], which keeps interventions from upper management to a minimum during the initial stages and anticipates only a limited number of recommendations and adjustments for this period.

The remainder of this document is structured as follows. Chapter 2 introduces some terminology and outlines the scope of this study. We first explain why assessment and performance monitoring are treated as related, but separate tasks. Then give an overview of the core aspects under assessment, accompanied by short comments on the methods used for their investigation.

Chapter 3 reframes SPARTA's central aims and working agenda, accounting for shifts of the research-political context since the call for proposals in October 2017, and discusses their alignment with the technological and institutional landscape of 2020. This discussion serves as a baseline for assessing the pilot both within and outside the constraints imposed by the original set of KPIs defined in the DoA.

Chapter 4 outlines structural features of the SPARTA pilot: WP types, single WPs, and tasks within WPs. We briefly introduce the elements of SPARTA's governance structure, analyse their envisaged roles and contrast them with the practices and processes that have evolved during year one. We discuss the pros and cons of keeping the structures for project and the pilot governance aligned, motivate why we distinguish project management and pilot governance related objectives, and describe the implications of this distinction for pilot assessment and project monitoring. After recapitulating the fundamentals of SPARTA's governance structure, we describe the main aspects of its practical operation in year one.

Chapter 5 covers the actual assessment in seven parts. Part 1 is based on findings from a survey amongst SPARTA partners. Part 2 applies the general objectives from the SU-ICT-03-2018 call as assessment criteria. Part 3 lists the tasks specified by the call, and part 4 isolates the subset of DoA-defined KPIs. Part 5 estimates the current potential of the technical work packages for horizontal activities and as instruments for governance. Part 6 summarizes and comments on the free text comments received as part of our survey. The final part 7 revisits the process and results of assessing SPARTA's governance from a self-reflective and critical perspective.

Chapter 6 discusses the results, summarizes the findings, and presents our plans for the follow-up deliverables D1.4 and D1.6. In short, we aim at developing a prototype for framework that encompasses value-led governance, management and auditing. We hope this study and its follow-ups will help to achieve this goal.

At the end of this document, the reader finds a list of abbreviations, a glossary of terms, a bibliography, and three annexes. Annex 1 includes details on the questionnaire; annex 2 concerns the mapping between KPIs and Milestones. Annex 3 documents our (so far unsuccessful) exercise of extracting assessment aspects from the current list of risks continuously monitored by project management.

Chapter 2 Terminology, Scope, Approach, Methods

2.1 Terminology

Establishing a pilot for a CCN is an open-ended and experimental enterprise. Even partial failures may turn out to have value, and a thorough analysis of dead ends can prove valuable to avoid pitfalls when moving towards an institutionalized instance of a CCN and an ECCC. Success or failure as a project and success or failure as a pilot are therefore two different things. For this reason, this study draws a major distinction between *project* and *pilot* related matters and distinguishes *project monitoring* and *performance management* on the one hand from *monitoring* and *assessing pilot governance* on the other.

SPARTA can be conceived as having at least three major dimensions. SPARTA is:

1. A research *project,* subjected to the EC's rules for Research and Innovation Actions (RIA);
2. An experimental, living *pilot,* modelling a transnational organization with dedicated competency in cyber security Competence, a nub-spoke structure and network characteristics;
3. A potential blueprint or *template* for a future institutionalized European Cybersecurity Competence Network.

The first dimension corresponds to *project management* tasked to safeguard that SPARTA adheres to the rules for EC funded research. Progress is tracked against objectives defined by its *Description of Actions* (DoA) [16]. At annual intervals, progress is also checked against a number of quantitative key performance indicators (KPIs) that were defined at the beginning of the project.

The KPI figures reflect the initial ambitions; the success of SPARTA as a project is not predicated on achieving all of them in full. This observation applies even more to the other two dimensions of being a pilot and a possible blueprint. This observation motivates to maintain a clear distinction between *project management* and *pilot governance*. ***We emphasize that the purpose of D1.2 is to assess the governance of the pilot, not that of the project*.** That is, we are mainly assessing the pilot governance performed in the context of (WP1).

Progress tracking in terms of *project management* is a task in its own right primarily carried out by SPARTA's WP13 (WP2 specific aspects are also covered in depth by a dedicated, WP2 internal review process). It is part of *performance management,* primarily action-oriented, encompasses sensory and analytical as well as executive capabilities. It is based on the sub-task of *performance monitoring* which gathers the data points and translates them into figures digestible by management. Performance monitoring frequently has an analytical angle as well, but where this is the case, it tends to operate on the basis on well-established categories that can be linked to indicators and metrics easily understood by decision makers. If performance monitoring is carried out on a regular basis, it can enable more abstract metrics for predictive, model-based evaluation against well-defined future objectives.

Assessment makes use of data from performance monitoring, but treats it as just one among other sources of information. However, it also tries to contextualize governance objectives, and it may devise a suitable, extended set of categories and indicators for this purpose. Initially, assessment and monitoring indicators may be tentative and of merely qualitative nature. Performance monitoring may or may not always include analytics, but it always leverages existing process knowledge to supports managerial tasks. Assessment is open towards categorically new insights, thereby supporting objectives at the executive and governance level.

2.2 Scope

For the purpose of this study, *assessment* is the encompassing activity, leveraging *performance monitoring* as a sub-discipline where so required without extending into *performance management*. The following aspects are **inside the scope** of the assessment:

1. *Selected elements of the research-political context*. These are of essentially "external" nature, so their natural place would be the year-two deliverable D1.4. However, some of these aspects have influenced SPARTA's approach for governing the CCN pilot, and they continue to do so. This is why we have included them, notwithstanding that the focus of this study (D1.2) is the assessment of pilot-internal affairs from an internal perspective.
2. *Assessment of pilot governance activities* carried out in the context of WP1.
3. *Occurrence of planned and unplanned interactions* across WPs, tasks, technical and non-technical strands of work, and individual partners (encouraged in the DoA).
4. Self-reflective "assessment of assessment" -- depth, continuity, and quality of indicators.

In contrast, the following aspects are **beyond scope**:

5. The assessment of day-to-day technical and organizational project management covered by WP13.
6. The assessment of progress of the R&D&I work packages (as tracked by WP13)
7. The assessment of Dissemination and Exploitation activities (WP11, WP12). These are primarily project rather than pilot-oriented activities (tracked by WP13).
8. Details on monitoring the performance monitoring of WP2 (see D2.2 for this)
9. SPARTA's agility and responsiveness to adopt tasks beyond the DoA-defined ones. No corresponding initiatives have occurred during the reporting period.

2.3 Approach and Methods

Elements of performance monitoring are included by selecting those DoA defined KPIs that support the assessment pilot governance, as are suitable methods employed by T1.2 and T1.3. These are extended or complemented with results from data mining, questionnaires and interviews[2]. This yields a subset of assessment indicators of mostly qualitative nature. One of our aims for future studies is to make this subset compatible with structured, quantitative, industry grade methods for assessment already applied by SPARTA partner INOV in the context of WP2.

For our assessment, we will proceed as follows:

1. We first re-construct the research-political context by revisiting the political declarations, the call for research on CCN pilots, SPARTA's DoA, and the Considerations on COM(2018)630 that were or have become relevant for shaping the project. This is complemented by a high-level outline of the current cyber security landscape with focus on recent developments that may have consequences for the organization, scope, and focus of a real-world CCN and ECCC.
2. The assessment of pilot governance activities starts with gathering data from the project's DoA, the document management system, topical mailing lists, and web server. To clarify specific details, we rely on agendas and minutes of board meeting and events coordinating WP activities, the quarterly progress reports, or memos for events targeting SPARTA affiliates or the wider community. These are complemented by the information from structured interviews, questionnaires, and pilot-specific KPIs defined by the DoA.
3. The assessment of pilot-internal interactions is based on the results of an internal survey and structured interviews. Where required, it can be complemented by data from SPARTA's management support system.
4. Assessment, including its self-reflection, assumes a pure T1.4 / WP1 perspective. In the spirit of the title of this deliverable, it is presented in a "lessons-learned" format. In order to alleviate the "observer problem" created by introspective self-reflection, this study will, at some later stage, be subjected to an independent appraisal of SPARTA partner ISCOM, who acts as an advisor and independent monitor for the T1.4 assessment process.

[2] Datamining was employed to determine the number of monthly messages to SPARTA's various internal mailing lists. This could be performed in a fully anonymised way that solely relied on the time and date information of the messages sent. In the case of the questionnaires, all data elements identifying individuals and all free-text comments were stripped from the datasets prior to statistical processing. The free-text comments were anonymized in terms of the individuals and the organizations submitting them. This information was replaced by a numeric identifier. This allows tracking common provenance across different comments.

Further to the tasks described above, we are experimenting with methods for tracing interaction patterns between SPARTA partners or for determining their degree of alignment to SPARTA's governance structure and processes. The experiments are carried out as part of ongoing research on applying methods of network analysis for building a CCN pilot governance "dashboard": a decision support system for finding governance bottlenecks and hidden potentials for co-operation across WPs, tasks, and partners. This research is in its early stages; we hope to present first results as part of the assessment for the next working period.

The remaining part of the study is interspersed with highlighted sections containing aspects we believe to be of importance for the governance of the pilot, which can also be found in a thematically grouped list at the end of the last chapter. The following simplified diagram depicts the sources, processes and results from chapters 4 and 5 for the detailed assessment of SPARTA's pilot can be found.

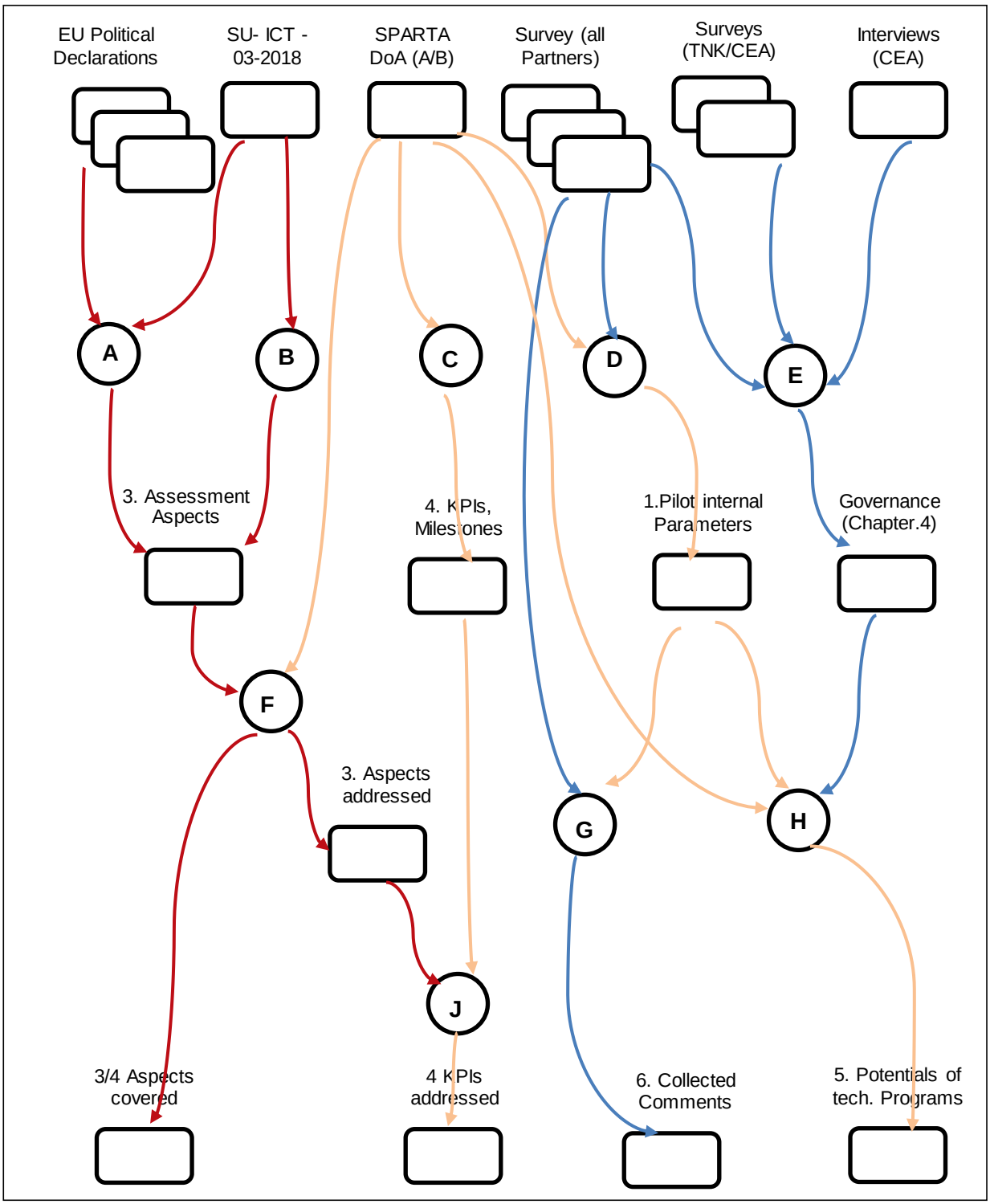

Figure 1: Assessment Workflow -- Table: Assessment Single Tasks

Assessment : Single Tasks					
A	Isolate Objectives	D	Involvements & Dependencies	G	Categorize / Summarize
B	Isolate Tasksk	E	Governance Design & Practice	H	Summarize / Taxonomy
C	Isolate KPIs and Milestones	F	Assess Coverage	J	Match / Assess Coverage

Chapter 3 Research-Political Context

SPARTA's first annual working period was characterized by uncertainties about the scope, institutional positioning and interaction model of a future European Competence Centre for Cybersecurity (ECCC), the European Cybersecurity Competence Network (CCN), and single National Cyber Competence Centres (NCCCs). We therefore start with a discussion of the research-political landscape for cyber security in Europe, highlighting a number of factors influencing the selection of appropriate objectives for governing SPARTA as a pilot.

Initial EC announcements [1] on plans for a new European Cyber Security Agency *to assist Member States in dealing with cyber-attacks* [2] go back to the Juncker address from September 2017. The goals stated by him have since been endorsed and extended by the new EC presidency. In September 2019, president elect von der Leyen reemphasized the need for unified approaches to cyber security, including certification, knowledge sharing, and a common platform in the form of a new European agency.

Until recently, the governance model for such an agency was mainly conceived as a network of national entities to be nominated by the member states. The preference for this model has only recently been backed up by an empirical study [12]. Cyber security practitioners were asked about their opinion on the most suitable governance model for such an institution. A substantial majority held the view that the flexibility offered by a network of national entities would best reflect the high dynamics of cybersecurity. Two alternatives, namely the hierarchical or market-driven approach, were considered as too static and too erratic, respectively. The preeminent objective of European Cyber Security initiatives was seen in *coordination*, while *transparency of decision-making*, *trustworthiness* and *resilience* are considered as the primary areas that require most improvement.

According to named study, *ENISA* and the *Data Protection Authorities* are viewed as the two *key institutional players* in the cyber security realm at European level, with *CERTs* in third place. When asked who would be best placed to select the institution operating a national cyber competence centre (NCCC), most respondents thought that the member states, and not the European institutions, should make this call.

However, when it came to the role of a future European CCN, the study found no consensus. Opinions varied widely whether this agency (1) should *focus on technological* or on *other measures*, whether (2) it should push different *national centres* towards *specialization* or not. There was also no agreement on (3) whether this institution should push *mandatory cyber security certification*, and whether (4) a European Competence Centre for Cybersecurity should limit its role to just *distributing funding* and supporting technological innovation. In terms of criteria for choosing between major governance alternatives for CCN pilots such as SPARTA, the findings of the study offer no guidance.

Anticipated roles of ECCC and CCN

A European Competence Centre for Cybersecurity is thought to have the primary objective of supporting the development and rollout of the tools and technology required to keep up by including the shifting threat landscape [3]. However, the EC's proposal also includes tentative ideas of extending the role of this institution towards the field of internal (police, emergency services) and external (military) security. The corresponding political declarations and the SU-ICT-03-2018 encourage to ponder the following options:

- including cyber defence within the (voluntary) Framework of Permanent Structured Cooperation (PESCO) and the European Defence Fund [3],
- cooperating with NATO in coordinated exercises and in fostering cyber defence research,
- further developing the planned European Cybersecurity Research and Competence Centre with a cyber-defence dimension [ibid],
- allowing research and innovation dual-use cyber technologies in CCN research [4],
- approaching EUROPOL and agencies other than DG_CNECT as partners for co-operation and for outreach [ibid].

When assessing governance options for the CCN pilots [7], one cannot exclude a potential ECCC role within an evolving trans-European security architecture. This does not simplify the quest for an appropriate governance model, because carefully guarded domains of national sovereignty are involved.

It is mostly uncontroversial that growing interdependencies between the civilian sphere and the one of national defence call for integrated strategies when it comes to critical infrastructures protection and cyber defence. On the other hand, initiatives in favour of streamlining or mixing concerns of internal and external security tend to be met with serious and well-founded reservations from many quarters. These concern increased difficulties for parliamentary control, the blurring of boundaries between civilian and non-civilian realms, and well-known tendencies for closed-shop practices, dictated by standard operational practices of the intelligence, police, and military services. Finally, there are objections because the cyber defence landscape might be fragmented even further: there plethora of executive authorities already exists [6].

We emphasize that the Cybersecurity Act -- *Regulation (EU) 2019/881* -- and the proposed Act for a European Cybersecurity Competence Centre and the Network of National Coordination Centres -- *(COM(2018)630)* -- were intended to address different regulatory realms. From a governance perspective, structures and processes would be simpler if the role of the ECCC would be confined to research-related matters.

3.1 National Competence Centres

European countries have rather different ways of mapping cybersecurity in their national institutional framework. The current design of a European Cybersecurity Competence Network assumes each country will nominate its preferred candidate to operate its national coordination centre [5]. This is likely to lead to problems. There are governments pursuing a centralized cyber security strategy such as France or Lithuania, for whom such a nomination might be relatively straightforward. In contrast, countries following a federated approach may be hard pressed to find a suitable institution among multiple candidates with different focal points and competence levels.

The European Cyber Competence network is primarily designed as an entity to support research, and not all national candidates may have capabilities for fruitfully interacting with the ecosystem for research and innovation[3]. The CCN pilots will have to investigate governance options for a European competence hub (tasked with initiating and co-ordinating cyber-related R&D). But they also cannot disregard the prospects of having to interact with national counterparts whose skills and competencies may vary widely[4].

When comparing the cybersecurity strategies of selected EU member states in a preliminary internal study [8], first results indicate that the implementation of the NIS Directive by these states has not led to any level of uniformity at administrational or organizational level. The only common denominator we could find was the existence of a national CERT in each country.

Given this state of affairs, none of the four CCN pilots can hope to find a governance model that fits the needs of all European member states. As a fall-back strategy, exemplary models for selected national clusters could be designed, preferably for countries strongly represented in a CCN pilot. For SPARTA, this would apply to clusters from France, Lithuania, Italy, and Germany.

In theory at least, SPARTA is in a position to synchronize similar efforts between all four pilots, as some of its resources are specifically allocated to governance assessment. This would concern a governance model that assumes national entities are responsible for passing on EC funding as they

[3] E.g., in Germany, possible candidates include: (1) NCAZ (German Cyber Defence Center, Home Office, Bonn), (2) NAIC (envisaged National Agency for Innovation in Cyber Security, Home Office and Ministry for Defence, Halle/Leipzig); three nationally funded Cyber Competence Centres -- (3) CISPA, Saarbrucken, (4) CRISP, Darmstadt, (5) KASTEL, Karlsruhe, all Ministry of Education and Research, and three independent Cyber Competence Centres / Clusters of national importance -- (6) FKIE, Wachtberg/Bonn, (7) CODE, Neubiberg, and (8) HGI, Bochum,.

[4] An EC hearing with a consultation of the CCN pilots (amongst other stakeholders) on this specific topic was scheduled for mid-January 2020.

think best. The *Considerations on COM(2018)630* ratified by the European parliament allows EC funding to be passes through cascading grant agreements [5]. This enables national competence centres to pursue their own research agendas with funds the EU. The model stands in some contrast to the one currently implemented by SPARTA, which assumes a central European institution which is capable of co-determining the research directions through open leadership and participative decision-making.

3.2 Focus and Scope of the Pilot

Eventually, it will be necessary narrow down the scope and focus of the SPARTA pilot. Many, but not all criteria for guiding this choice can be gleaned from the wording of the original SU-ICT-03-2018 call. Others rely solely on the preferences of the consortium. However, the most important decision criteria will be provided by the research-political realities on the ground.

Sharpening the focus of a CCN pilot can be achieved by reducing its scope to concerns that exclusively regard topics covered by DG-CONNECT. This strategy would imply ignoring horizontal themes involving multiple DGs. Alternatively, the consortium make the choice of exclusively focusing on the requirements of a well-defined group of stakeholders. What comes to mind here first are organisations with operative capabilities: military, police intelligence services, civil emergency task forces, and security-critical verticals such as aerospace or defence. However, focusing on these stakeholders alone would deliberately ignore more generic challenges posed by ubiquitous IT, the Digital Transformation, and not least the Digital Europe programme. This self-limitation would also pre-empt political decisions yet to come: as of January 2020, the role and tasks of a European CCN is still a matter of an ongoing debate.

3.3 European Security Certification Scheme

We are currently observing a political push for introducing a scheme of voluntary or mandatory IT security certification at European level[5]. The proponents of this idea maintain that it is possible to create a regulatory instrument helping to establish, at least in the medium to long term, some baseline for cybersecurity, at a level that still has to be technically specified. This idea is not without merits. After all, certification schemes have been successfully employed in fields like avionics, pharmaceuticals, electrical goods or financial services. It therefore stands to reason that they are considered a regulatory option for cybersecurity. Consequently, all CCN pilots are expected to advance the case for certification by researching technology for the testing and validation labs of the responsible national authorities with state of the art technologies and expertise [4].

Regarding topicality, it could be argued that IT validation and certification as well as research on these topics falls exclusively under the responsibility of ENISA and the DG-CONNECT, respectively. However, the mandatory cyber security certification would have repercussions far beyond DG-CONNECT's realm[6]. From the perspective of governance, SPARTA is therefore well advised to

[5] See *Regulation (EU) 2019/881 Of the European Parliament and of the Council of 17 April 2019,* in particular Title III

[6] E.g., it is likely to have immediate consequences for innovation and competitiveness, may raise the bar for entering this commercial segment, accidentally erect trade barriers, could reduce desirable flexibility in responding to cyber threats, and undermine corporate strategies for tailored assessment, management and insurance of cyber related risks.

ensure that corresponding activities neither advance nor rely on regulatory preferences[7] for introducing mandatory certification across the board.[8]

3.4 Ethics and Socially Responsible Research and Innovation

Cybersecurity is plagued by ethical and societal problems in more than one regard, and this observation applies to research in this field as well. These problems are rarely mentioned, and discussions tend to be confined to informed conversations, closed committees, and fringe conferences. This further contributes to an often-deplored fragmentation of research, development and market. Cybersecurity is an intersection of stakeholder communities whose motivations and interests can be different to the point of being incompatible, irreconcilable, or even adversarial.

To illustrate this point, it suffices to name just some of the players: national agencies and whistle-blowers, law enforcement authorities and defenders of privacy, academic researchers and white-hat hackers from the fringes of cyber-society, military or intelligence services, and adherents of policies for transparency and full disclosure. This diversity leads to potentially contradictory goals in statements and calls issued by EU institutions (see section on the anticipated role of a European Network for Cybersecurity Competence above).

It is anything but trivial to establish a hierarchy of values here that will be accepted by everyone. Take the question of digital autonomy, which constitutes an ethical matter in itself with regard to the values and governance of European society. It not only concerns questions about the desirable and practically achievable degree of autonomy for implementing and operating cyber security infrastructures and platforms on behalf of prosecution authorities and cyber warriors from the armed forces. In equal measure, this also concerns the absence of adequately secure platforms for the great European public and European enterprises. As far as it regards underlying hardware, cloud data storage and processing, web searches, and social media, Europe's reliance on infrastructure not invented here is blatantly obvious. This leads directly to the enormous flows of data across Europe's regulatory boundaries, where options for regulating the behaviour of the operating entities are severely constrained. The deplorable state of affairs could be considered as a wake-up call to Brussels for actively creating technical alternatives closer to home.

There are other prominent examples of cybersecurity aspects that come with an ethical angle that will eventually have to be addressed by analysis, political debate and regulatory initiatives. To give just a short list:

- Methods for enforcing constraints on certain types of information in the face of conflicting demands from civil society for uninhibited and uncensored access to information of public interest;
- Methods for digital surveillance and tracing in the interest of national defence or criminal prosecution in the face of threats to privacy and protected business communication;
- Methods for retaining data for auditing or historical research, and the right to be left alone or being forgotten,
- Methods for predictive and proactive cybersecurity and the expectations of law-abiding citizens that they will not be unduly scrutinized.

Ethical triggers may originate from more unexpected quarters as well. Take the matter of ecological sustainability: many mechanisms vital to cybersecurity are very costly in computational and energetic

[7] To name three of these aspects: (1) There is a lack of empirical evidence for a notable improvement of software quality by virtue of passing common certification schemes at various levels, in particular in comparison with other software engineering methods [9]. (2) A "once and for all" certification strategy [10] is typically adequate for long-lived physical goods with a standard safety lifecycle. Its applicability to the short-lived security lifecycles of frequently patched online IT systems remains questionable on principle grounds [11]. (3) From a practical point of view, mechanisms and procedures are required to reduce the prohibitive costs for (re-) certification by at least one order of magnitude.

[8] *Regulation (EU) 2019/881 (Cybersecurity Act)* makes provisions for voluntary certification and, in particular conformity self-assessment for "basic" assurance level. A principled, "open" approach to certification could make it its mission to provide tools, mechanisms and methodologies for pushing self-assessment towards the "medium" level.

terms. Choices of hardware architecture, programming language, execution environment, and platform as well as infrastructure design have significant impacts on the environmental footprint. This applies even more to cybersecurity mechanisms relying on large-scale data-mining or continuous training of extended artificial neural networks. In all these cases, questions of mere technical feasibility and pragmatic efficiency become overlaid by value-guided ones.

It is beginning to sink in that questions of sustainability questions extend beyond the socio-technical and economic realm. Consideration of this kind shed, among others, a new light on the often-deplored "skills-gap" in cybersecurity. Some 40 years ago, IT security, as it was called back then, was a marginal topic, of interest only to small groups of military personnel, civilian system administrators, and the fringe scene of early hackers. In 2020, it has evolved into a fully-fledged academic discipline, a thriving research ecosystem, dedicated governmental agencies, a market size of tens of billions of dollars, and a multi-trillion dollar damage potential.

During the last decade, the growth of cybersecurity disciplines has been astonishing. However, how fast and how far do we really want to see this sector grow? From the current 5%-10% of professional software development[9] to twice this size within a decade? Would this require co-opting initiatives from the civilian or the fringe spectrum[10]? What about the feasibility of pursuing socially acceptable and responsible innovation in cybersecurity, if these technologies also lend themselves to dual-use, intelligence gathering, or even "active measures"?

Pushing this argument even further: Cybersecurity is expensive. What is the acceptable premium, at societal scale and in terms of the percentage of the overall expenditure on IT or the GDP that should be spent on cybersecurity -- procurement, training, technical resources (CPU power, memory, storage, network bandwidth) and operating costs? If 100% of GDP is out of the question, would a hundredth of this be acceptable? Or 0.01%? Can such a figure be determined at all, and would it be suitable for guiding future decisions on the allocation of cybersecurity research funding by the EC in general and for a European Cybersecurity Competence Centre?

This raises related questions about technology choices and criteria for what can rightfully be considered as innovative in cybersecurity. Many "innovative" solutions in this field have a marked tendency of adding to the complexity that already exists. Is this evolutionary path without alternatives? Might there be another evolutionary strategy predicated on deliberately reducing complexity? What are the security objectives that could be tackled successfully by pursuing radical simplification? And: what would be the costs -- in terms of convenience, social acceptability, reactiveness, safety, but also for some currently attractive business models?

Concerns of this nature are likely to influence the choices about the governance of the CCN pilot, the focus of horizontal activities, including WP2, and topics to be addressed as part of the next assessment cycle and the corresponding M24 deliverable D1.4, appropriately titled "Lessons learned from externally assessing a CCN Pilot".

[9] A conservative estimate, not factoring in an estimated skills gap of up to 50%

[10] Some of these initiatives run at expert level. Their growing relevance has recently been documented by the remarkable figure of 17,000 visitors at the 2019 Chaos Communication Congress in Leipzig, Germany, see https://de.wikipedia.org/wiki/Chaos_Communication_Congress

Chapter 4 Characteristics of SPARTA Governance

This chapter starts with outlining the structural features of the SPARTA pilot: bodies, roles, WP types, single WPs, and tasks within WPs. Next, we document features, practices and processes that have evolved during the first year of the pilot, and compare them with the configuration anticipated by the DoA. In this context, we discuss the advantages and possible drawbacks of keeping the project governance structure aligned to that of the project.

4.1 The SPARTA Governance Structure

For reasons of easier readability, this sub-chapter recapitulates the description of the SPARTA's governance structure from the DoA part B V1.0. Readers who are familiar with the DoA can skip the section in italic.

"*Governance ties together the first two instruments and supports the network's research and innovation activities. SPARTA's governance structure recognizes leadership and diversity as powerful principles, and instantiates them in the following organs:*

- *The **Strategic Direction** coordinates the governance; in particular, it supervises the execution of the network's missions and assigns roles in the organization to ensure it stays true to its core principles. It validates the research programs based on the roadmap and on strategic priorities. It coordinates the Program Leads, monitoring progress and risks, incentivizing collaborations both within and across programs. The Strategic Direction monitors the progress of the Roadmap and of the Partnerships, and ensures the Taskforces are being fully associated.*
- *The **Roadmap Committee**, headed by the SPARTA Scientific Director, is in charge of the Roadmap as described in Instrument 1. It proposes the Program Leads to the Strategic Direction, based on strands of interest in the Roadmap, and assists them in extracting research programs from the Roadmap. Program Leads combine a recognized scientific and technical expertise in this strand, with an open-minded approach to problem solving, allowing them to evaluate promising concepts regardless of their field of origin.*
- *The **Partnership Committee**, led by the Partnership Director, handles the design and maintenance of the network's partnerships, including the Associates Council. It sets ups space, time, and means to enable research collaborations, leveraging the strengths of existing structures and organizations. As such, it takes the operational lead in the organization of the SPARTA workshops, supported by the Taskforces and the Associate Partners. It also creates and updates the map of platforms and infrastructures – pivotal in focusing data, software and expertise resources – based on a rigorous evaluation of the provided human, physical, digital, and virtual capacities; it finally ensures their coordination in serving the interests of European research and innovation teams.*
- *The **Training and Awareness Taskforce**, under the direction of the Training and Awareness Officer, provides expert inputs on the state-of-the-art, gaps, and advances in the field of cybersecurity skills development. It is instrumental in identifying coherent approaches to a harmonized, European-level cybersecurity training syllabus. It provides insights on the process and tools required in these fields, and helps identify potential areas of the Roadmap and Programs that can be of interest in building these capacities.*
- *The **Certification Taskforce**, under the direction of the Certification Officer, provides expert inputs on the state-of-the-art, gaps, and advances in the field of cybersecurity certification. It provides insights on the process and tools required in building next-generation certification tools, and helps identify potential areas of the Roadmap and Programs that can be of interest in building these capacities – either directly through progress in evaluation and conformity, or indirectly through advances in the development of specific security functions.*
- *The **Dissemination Committee**, under the direction of the Dissemination Officer, provides communication expertise and tools for the network. It ensures these tools are available across project boundaries, that communication exploits state-of-the-art (in particular digital) mediums while taking place in full respect of the constraints of the field and its practitioners.*

- *The **Ethics Committee** addresses the major ethical, legal and societal aspects relevant in the context of large-scale cybersecurity research and innovation in transnational competence networks. It pays particular attention to the topics addressed in the four SPARTA programmes but also investigate the insights' broader relevance for the cybersecurity research and innovation community. Considering the activities in SPARTA, it sets up and maintains appropriate procedures, criterias, templates, information sheets, potential opinions and approvals from relevant entities, explanations, and relevant compliance documentation as well as descriptions of technical and organizational risk-mitigation strategies and measures (including security ones) implemented to comply to the ethics requirements."* [16]

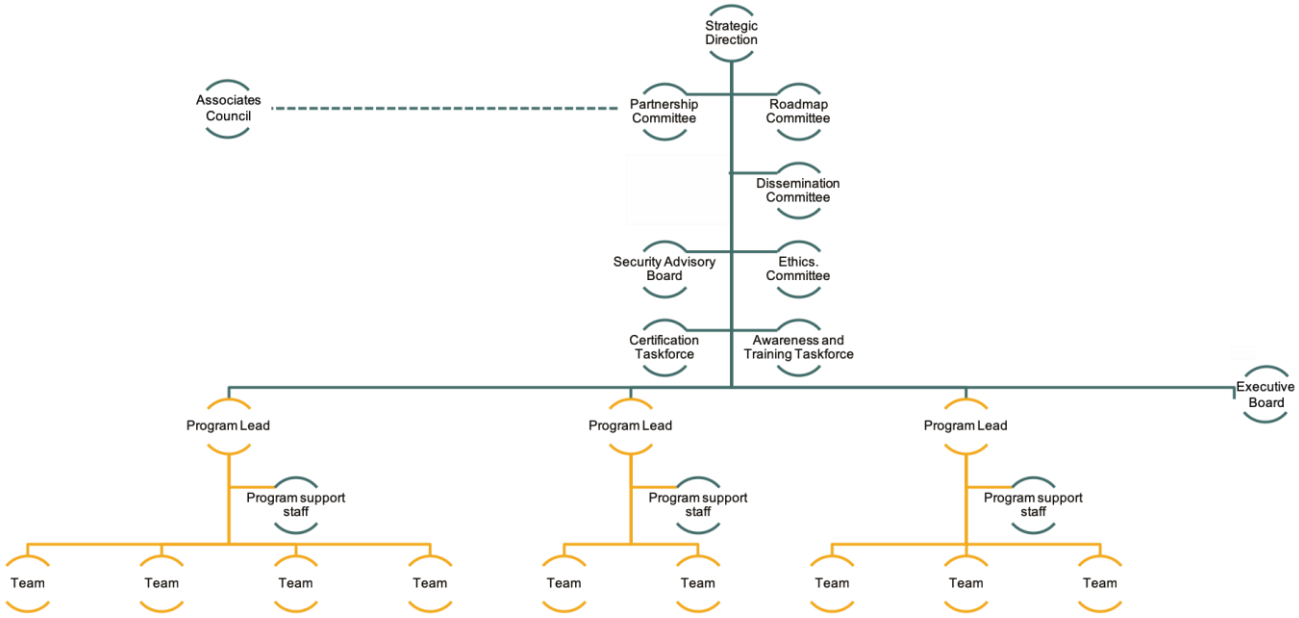

Figure 2: Organizational structure

4.2 SPARTA Pilot and Project Governance in Practice

The following two sections are based on semi-structured, in-depth interviews with a junior staff member and the Technical Director, both from CEA, who is tasked with the technical directorship of SPARTA. These face-to-face interviews lasted 60 and 90 minutes, respectively. They were based on two sets of questions unknown to the interviewees. The 12 questions in the first interview mainly focused on project management, the 15 questions in the second one on governance aspects for the CCN pilot. The replies were transcribed from the audio recordings into excerpts with summarized statements. The tags in square brackets of the following sections correspond to tags in these excerpts. They approximate the time when corresponding remarks were made during the oral interview.

4.2.1 SPARTA as EC Project

Project-related governance mostly involves coordination tasks such as preparing regular conferences of the executive board [[17]-13:00], agenda planning and invitations for external events and reviews [[17]-13:00], the production of corresponding information material, and the tracking of deliverables, and risk-management.

During the first year of the project, about half of governance effort was spent on DoA defined tasks related to mid- and long-term objectives. The remaining effort had to be spent on short-term issues such as external requests [[17]-19:30], deliverable-related "sprints", or additional effort required due to the temporary unresponsiveness of some partners [[17]-21:30]. During the first year, progress

reporting per partner occurred in monthly intervals. From 2020 onwards, this will be relaxed to quarterly reporting [[17]-25:30].

Editorial tasks are split between the technical lead CEA (content) and the organizational lead TNK (formatting) [[17]-23:30]. TEC also manages the mailing lists, the GitLab repository [[17]-30:00] and amendments to the DoA [[17]-28:00]. These tasks typically do not require the direct involvement of SPARTA's technical director.

CEA's and TNK's interactions with the SPARTA consortium tend to concern the members of the executive board; their intensity depends mainly on the schedule of deliverables. During the first six months, most interactions concerned management (TNK) and road-mapping efforts (TUM, INRIA) [[17].33:00]. The first version of the roadmap was finalized just in time to be presented in the EC's open consultation from EC, thereby ensuring a certain level of strategic impact [[17]-43:15].

From month 6 onwards, the focus of CEA's interactions shifted towards the WP4-7 leads for the technical work packages. So far, cross-WP issues have occurred that would have required intermediations from L3CE [[17]-44:30] and INOV [[17]-45:30] who are tasked with monitoring the technical programs resp. non-technical activities from a generalized perspective.

From a project management angle, adherence to the EC's funding and evaluation rules is essential for successful reviews; the "project" aspect of SPARTA is considered to dominate all other activities and results. Viewed from this angle, it is preferable to follow the DoA defined planning as closely as possible [[17]-58:00]. Overall progress is considered to be good; gear changes are expected for several area of work that required substantial preparatory work, namely the certification related activities, methodical interactions between non-technical and technical tasks, and innovative, and non-technical approaches to central pilot challenges.

Since the launch of the four CCN projects, the EC has made some effort to remind them of the importance of those aspects that sets them apart from ordinary Research and Innovation Actions (RIAs). All pilots are expected to produce roadmaps for future cybersecurity technology, but to chart unknown political and organizational territory as well. It is indeed true that expectations of this kind chime through the SU-ICT-03-2018 call [3] and were expressed in the *Considerations on COM(2018)630* [5]. However, not all of these challenges were mandatory and had to be adopted in the CCN proposals. In particular, shouldering new tasks in addition to those already committed to was not one of them. Within the constraints of their resources, SPARTA's management is already stretched to a point where taking on any additional burden could cause serious difficulties for CEA and TNK. [[17]-50:15] Unfortunately, this also limits SPARTA's options of testing the pilot's agility and capability of adopting new technical challenges "on the fly".

4.2.2 SPARTA as CCN Pilot

Pilot-oriented governance concerns the continuous re-alignment of SPARTA efforts with the evolution of CCN pilots in general, reaction to shifts in the research-political context, the adoption of new technical directions, and objectives that cut across work packages. The corresponding WP1 includes a dedicated task T1.4 for continuously monitor the adequacy of its operation in an attempt to design a governance structure that extends beyond the duration of the project [[18]-00:00:10]. It also acts in a facilitating capacity as an independent observer and collector of comments during coordination meetings [[18]-00:02:00], and in supporting the evaluation of new ideas through a process of agile and friendly feedback [[18]-00:04:00].

SPARTA's approach to internal governance attempts to meet the requirements of both project and pilot management simultaneously; the underlying governance structure is identical. In practical terms, members of the Executive Board (EB) address project related matters, such as interactions with SPARTA's general assembly, the European Commission and the Project Officers. Pilot related issues are concerns of the Strategic Board (SB). During SPARTA's first phase, the project's EB has provided the interface between project and pilot. The pilot may eventually install a dedicated EB once its activities start to get traction [[18]-00:22:00].

Steering a pilot and a prototype for a future institutional set-up within the regulatory framework imposed by the rules for EC funded projects poses a number of serious challenges. Resources have

to be allocated right from the outset, which makes it difficult to reserve parts of the project budget for yet-undefined future activities. Internal re-allocation of resources is possible but may require a change of contract to be endorsed by the legal departments of more than 40 SPARTA partners, making this a theoretical option at best. Similar considerations apply for the option of progressively releasing payments to the consortium partners, since this would overwhelm the accountants. In summary: for a project of SPARTA's size, there is little room for changing tasks and structures, replacing partners for new ones as soon as responsibilities have been assigned and resources have been allocated [[18]-00:24:00]. The flexibility for incentivizing experimentation, the adoption of new tasks and the discontinuation of stale ones, is thereby much reduced.

Historically, the initial core group of SPARTA comprises several national clusters which initially considered independent proposals, but decided to join efforts in a comprehensive working agenda [[18]-00:09:10]. In addition, many partners have worked together in previous research collaborations, which allows to exploit existing social capital. As a result, some parts of the pilot have operated in a networked way from day one [[18]-00:36:00]. On the other hand, the main transversal activity of this work period-- the production of the roadmap -- relied heavily on centralized steering and control mechanisms. The plan for the upcoming periods is to delegate similar tasks wherever feasible and to foster areas of partial technical autonomy. This will require intermediaries at lower management levels to step in [[18]-00:45:00].

Beyond a project-focused perspective, pilot governance involves monitoring the shifts in the research-political landscape, to accommodate evolving stakeholder expectations, and to honour EC requests of strategic importance. During the first working period, numerous requests of this type have reached the Technical Lead of the SPARTA pilot (e.g. concerning the synchronization between activities of the various CNN pilots, research roadmaps and "moonshot" initiatives for cyber security research, or scoping future national competence centres). This has led to project-internal concerns about feature and expectation creep; being caught out or overtaken by the development at the research-political front figures prominently on SPARTA's list of closely monitored risks.

To counter this risk, the SPARTA consortium will have to make some stark choices for the upcoming periods. Based on a widely agreed rationale, it has to settle on a small set of questions to be addressed in future, both for the technical programs and for the transversal activities such as certification, training, governance, and social aspects [[18]-00:50:00].

For the time being, interactions with SPARTA's Advisory Board will remain at a reporting and consultative level [[18]-01:01:00]. The main exploitation strategy for the technical program is to present SPARTA's concepts and ideas to the market in general and to the associates in particular to test their validity, and hopefully, to spark interest in adopting them,. To this end, initial demonstrator activities of the programs have served an important purpose [[18]-01:10:00]. However, there are no current plans to create new spin-offs or start-ups [[18]-01:07:30]

SPARTA's model of interacting with external partners adopts a 3-tier model of "friends", "associates" and "network members". The current policy is that every "well-intentioned" (non-hostile) organization should be acceptable as an associate who can commit ideas to be reflected in the roadmap [[18]-01:11:50]. As of Dec 2019, there are no plans or initiatives for involving associates in research activities directly, to co-opt them for complementary proposals [[18]-01:01:00], to supply a common technology platform or to offering consultancy services to them. In general, the pilot governance model shuns options of preferential treatment; access to platforms SPARTA may produce in future should not be based on being a SPARTA associate [[18]-01:11:50].

A delicate aspect of SPARTA's pilot governance activity is related to the interactions with other CCN-related initiatives [[18]-01:19:00]. This not only concerns the *Ifs* and *Hows* of synchronizing and co-operating with the other three CCN pilots [7], but also interfacing earlier or parallel initiatives from ECSO. All CCN projects are poised to emphasize those aspects that are spelled out in the "agenda du jour" of the European institutions, while there is ample space for four distinctive CCN agendas with very few overlaps in target groups, stakeholders, geo-administrative scope, technical focus areas, and governance models. The issue at stake is to maintain one's own unique CCN signature while co-operating with other CCN pilots and projecting topicality and relevance, all at the same time.

4.2.3 SPARTA Governance in Year 1: Comparing Plan and Implementation

With the exception of the pragmatic separation of duties between the Executive Board (mostly dedicated to project related tasks) and the Strategy Direction Board (mostly focused on pilot specific matters), the original design of the SPARTA governance model corresponds to its practical implementation.

An EB activity dedicated to pilot related activities is likely to be launched once these -- and in particular, the transversal ones -- start to get traction. The amount of governance resources spent on honouring external requests was quite unexpected; it has reduced those originally assigned to pilot-internal matters.

Activity levels and impacts of the different organizational entities varied widely. This can be attributed in large parts (a) to the types of activities carried out during SPARTA's first period of work and (b) to the extended ramp-up time for the transversal tasks. Further details can be found in chapter 5.

The design of the structural entities (councils, boards, committees, and task forces) has proven to match the requirements of the project and the pilot. In a template for a future institutionalized CCN, the Dissemination Committee is likely to be replaced by a public relations entity. Apart from this, there are no indications so far that SPARTA's governance structure would require substantial adjustments to support a future ECCC.

Governance consideration: As a matter of contingency planning: develop a model for a weak ECCC interacting with national competence centres resp. clusters (see chapter 3). Consider elevating this objective to pilot governance level, e.g. by nominating a champion with a seat at the Executive and Strategic Board. Depending on the complexity of this undertaking, a task force may be required.

Chapter 5 Pilot Governance Assessment

Chapter 5 concerns the assessment proper. We first clarify the relation between project management and pilot governance and implications for pilot assessment and project monitoring. Based on the political announcements, considerations and the corresponding call SU-ICT-03-2018, we created a comprehensive, primary set of assessment monitoring aspects (AMA) that cover all the objectives and tasks defined in the original documents. We then assess each of these aspects with respect to their level of achievement.

We determine which of these aspects have already been addressed in full, either by provisions of SPARTA's DoA or by implementing them as part of pilot governance during the first working period. By removing these aspects from the primary set, we arrive at a secondary set of monitoring aspects that should be tracked not just for this working period, but on a regular basis (RAMA), and the set of aspects only monitored a single time (SAMA).

In a third step, we attempt to match the RAMA and SAMA sets against the set of DoA-defined KPIs for this working period. We thereby determine whether all relevant aspects correlate to KPIs and vice versa. "Orphaned" KPIs indicate a mismatch to the DoA, "orphaned" AMAs indicated that some relevant aspect of the DoA is not addressed by a corresponding KPI. The absence of any orphans indicates that all tasks required by the SU-ICT-03-2018 call are covered by the DoA-defined KPIs for this working period.

We re-emphasize that our assessment distinguishes *project management* from *pilot governance.* In particular, the actual achievement of specific technical objectives (which is tracked by the corresponding WPs 4-7 and WP13 is not a primary concern of ours. Instead, we assume a pure WP1 perspective that is oblivious to *technical and operational project management* matters addressed by WP13. Exceptions may be made if project management matters overlap with governance aspects, or if the boundaries between the two are blurred.

This study is produced in the context of task T1.4 and is an integral part of the pilot governance activities of WP1. We therefore include a self-reflexive element in assessing our own assessment of governance and a discussion of how it might be improved.

Part 1. Pilot-internal Parameters

To get a feeling for the current pulse of SPARTA, a questionnaire was sent to all consortium members in the second week of December 2019, to be completed by Christmas 2019 by a member of staff involved in the project. Follow-up requests were sent in early January 2020 to those whose answers were still pending, extending the deadline until Jan. 6. The requests were clearly marked as official governance request and sent out by the project managers. Still, we received only 38 answers on time, and two others after the cut-off date, preventing them from being included in the evaluation.

To maximize the chances of questionnaires being returned, and in adherence to the DoA that dictates keeping assessment method lightweight and flexible, we kept the number of questions to a minimum and offered answers as multiple-choice options wherever possible. The questionnaire and the datasets retrieved can be found in Annex 1: Governance Assessment Questionnaire 2019.

General Information

The questionnaire asks for the name, affiliation, and email address completing it. This allowed us to contact the sender if necessary. It also allows us to direct follow up requests to the same individual to enquire about perceived changes. Prior to the evaluation, the data sets were anonymized.

Building a core Group, getting involved, assuming Responsibility

To bootstrap a CCN pilot, and in particular to implement the equivalent of national clusters in its context, there is little alternative to starting from pre-existing networks of cooperation and trust. At a

later stage, this may translate into preferences for allocating roles and functions in the organizational structure of the pilot.

This observation motivated our question whether SPARTA partners considered themselves as members of the original core group conceptualizing the proposal, or whether they had joined later. We also enquired whether they had joined the project due direct request from the technical lead, or whether the first contact had been made by referral.

13 of 38 respondents (appx 40%) answered that they believed having been a member of the core group. Most of them had been invited by CEA directly, with the exception of CESNET and NCSR, who joined as the result of referral. The data suggests that 25 of 38 respondents (appx 60%) were invited by the project lead, while 13 (40%) joined after having been recommended.

The data suggests that becoming a member of the project and pilot steering group was *not* based on having been a member of the initial core group. 4 out of 12 seats on the executive and strategic boards (25%) are held by the 40% core group. However, 11 out of 12 these seats (>90%) are shared between the 60% of members whose introduction was not mediated (INOV being the only exception).

Governance consideration: The average number of MMs allocated to a board member organization for *all* tasks is 48MM, with INOV (45MM), FHG (35MM), and CETIC (26MM) below average. Most of the partners on the EB and SB have some leeway to reassign some resources if unexpected issues of management and governance need addressing.

Potentials for interacting with associates and CCN pilots

Synchronization and cooperation with the three other CCN pilots (*ECHO, CONCORDIA, CYBERSEC4EUROPE*) and external associates is carefully managed by SPARTA's Technical Leadership. The questionnaire data revealed that three consortium members (FTS, UNILU, PPWB) are also members of at least one other CCN pilot initiative, offering an option for interactions at second-tier level. Further, 12 consortium members who do not have a seat at the EB or the SB confirmed that they maintain direct contacts with at least one external associate or supporter, namely TCS, UNAMUR, UBO, UNILU, JR, FTS, TEC, ANSSI, NIC, KEMEA, DTU, and PPBW. Should interactions with other CCN pilots or associates intensify, these organizations could act as go-betweens.

Top Cross-Task Involvement			
Partner	**Tasks**	**Roles**	**WP-L**
33-L3CE	22	CW AS	4
12-TUM	21	WT S	3
1-CEA	20	CW S	1
27-CINI	18	W S	6
13-UBO	18	T S	
23-IMT	18	W	5
40-ITTI	18	W S	7
25-TCS	15	T S	
16-KEMEA	15	S	
4-CETIC	15	W T	11
43-INOV	15	W S	12
22-ANSSI	14	C S	
32-KTU	14	T	
41-NASK	14	AS	
20-TEC	13	T S	
35-MRU	13	T	
7-BUT	12	W	9
5-UNAMUR	12	TA	
10-FHG	12	W T	2

Table 1: Cross-Task Involvement

Beyond the Silos: Implicit and tacit Knowledge

Projects the size of SPARTA pose a formidable challenge for internal communication. This regards the updates of the consortium members on activities beyond their assigned tasks and work packages, or their understanding of larger shifts influencing the general direction of a project. Consortium members who contribute to multiple tasks and work packages have a natural advantage here: they are in a position to see the "big picture" using multiple sources.

This led to the idea to create a network map of informational nubs and nodes that exist implicitly, by virtue of the pilot structure, possibly without having an equivalent in the organizational structure. The actual map is still a work in progress; Table 1: Cross-Task Involvement illustrates the underlying idea. We use the number of different tasks a partner contributing as a metric. No work package has more than six tasks, so any number above this can be considered an indicator of involvement across WPs. It turns out that on average, each partner contributes to 11.7 work packages (sigma 4.8). The table shows all SPARTA members with

contribution levels above this value. It also indicates the variety of roles each partner assumes (W)P-leadership, (T)ask leadership, (C)oodinating capacity, (A)dvisory role and (S)cientific contribution.

Most WP leaders are above the threshold (NIC being the exception, WP 8 and WP10 unknown due to lack of data). As to be expected, the Technical Lead ranks near the top of the list. However, two of the partners are even further up the scale, and four of them have just two involvement points less than the lead.

According to this tentative metric, a number of partners operating at the second tier of the pilot outrank that of some WP leaders with comparatively few cross-task involvements in terms of well-connectedness. These partners are potential candidates to tackle more general, potentially governance related concerns, which are likely to intensify during the two upcoming working periods.

The lower end of the spectrum (involvement in 8 or fewer tasks) is not displayed here. Governance should take care to inform this set of partners about parallel activities in other WPs, relevant board initiatives, and the rationale for governance-initiated organizational adjustments that may be considered in future.

According to this metrics, there is at least one apparent mismatch between the level of allocated resources and the level of cross-task/WPs interaction. In this particular case, the partner commands substantial in-house capabilities and therefore may rely on cooperation with external partners to a far lesser degree than usual. From a governance and project management perspective, it may nevertheless be worth revisiting this issue.

Level of perceived dependency			
Partner	#Tasks	Dependency	WP-L
12-TUM	21	4	3
1-CEA	20	4	1
43-INOV	15	4	12
10-FHG	12	4	2
33-L3CE	22	3	4
22-ANSSI	14	3	
32-KTU	14	3	
5-UNAMUR	12	3	
24-INRIA	8	3	
16-KEMEA	15	2	
41-NASK	14	2	
20-TEC	13	2	
35-MRU	13	2	
14-UKON	10	2	
15-UTARTU	7	2	
17-NCSR	7	2	
34-LKA	7	2	
23-IMT	18	1	5
27-CINI	18	1	6
4-CETIC	15	1	11

Table 2: Perceived Dependency

The tentative approach presented here is part of an experiment to apply methods of social network analysis to SPARTA's governance structure and processes and to determine the feasibility of a CNN governance "dashboard". A possible approach for including additional parameters is outlined in the next section.

Governance consideration: When having to delegate governance tasks of more general nature, consider the list of "hidden champions" with high cross-task and cross-WP involvement. Be careful to inform partners with low levels of cross-involvement regularly and to a sufficient degree.

Interactions and Dependencies between Partners

For pilot governance, the actual level of interaction between different elements of SPARTA's organizational structure is of some interest. We therefore included corresponding questions, including one about the perceived degree of dependency on work by other partners, to be expressed on a scale from 0 to 4.

Our working hypothesis was that partners involved in governance (coordination, monitoring, advising) display markedly higher dependencies. The data suggests that this is indeed the case, at least for WPs with strong coordinative elements (WP1, WP2, WP3). This also applies if a leader of a technical WP assumes a role of cross-WP coordination and leads activities that include external involvements (as is the case for L3CE, leading a WP that implements playbook-based challenges).

Leaders of technical WPs appear to be less affected by dependencies beyond their control than leaders of non-technical ones. It is possible that the corresponding question was too ambiguous; it could have been misconstrued to gauge just the dependencies between technical objectives. We also consider the possibility that the questionnaire was completed by junior staff, who may have a

limited understanding of the various responsibilities of leading a work package and contributing at to decisions at executive and strategic board level. Still, the data suggests that some WP leaders feel to be less dependent on contributions than non-leaders, and even some indicated low levels of cross-task and trans-WP involvement, such as INRIA (4 WPs / 8 tasks), UTARTU, NCSR or LKA (each 3 WPs / 7 tasks). This matter may deserve some attention at governance level.

In this context, we note that the survey provides more data points to determine the interaction and dependency patterns than could be evaluated here. Whether a more detailed analysis can yield useful indicators for supporting pilot governance is a matter for future study.

The takeaway for SPARTA's pilot governance assessment is that there are a number of partners with a high level of self-perceived reliance on other members who have no direct means (such as WP leadership) and very few indirect ones (horizontal interactions) to communicate their situation. Depending on the criticality of tasks assigned to these partners, governance has to make sure that their concerns are taken seriously at WP level, and reach the EB and the SB in time. If necessary, special provisions should be made.

Chapter 4 and the first part of Chapter 5 should have introduced the most important structural and qualitative features of SPARTA pilot to a sufficient degree, so we now proceed with the more detailed, objectives- and task-oriented assessment.

Governance consideration: The T1.4 methods are currently too coarse to provide evidence for the actual existence of network-typical phenomena (horizontal interactions, dependencies, or build-up of social capital). They only work at a task and WPs level without accounting for individual contributors. Are complementary methods required here? Further, WP1 led assessment is only performed once a year. Should T1.4 type assessment monitoring be carried out regularly and more frequently?

Part 2: General Objectives of SU ICT-03-2018

The question guiding this part of the assessment is whether the structure and the process definitions of SPARTA's governance model (as defined by the DoA) and their actual implementation have been adequate to prepare for, execute on, or reach the following objectives:

1. Testing, validating and exploiting the possible organisational, functional, procedural, technological and operational set-up of a cybersecurity competence network with a central competence hub.
2. Building and strengthening cybersecurity capacities across the EU.
3. Providing input for the future set-up of the Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre.

1. To what extent has SPARTA tested, validated and exploited the possible organisational, functional, procedural, technological and operational setup of a cybersecurity competence network with a central competence hub?

To also reflect the early stages of the pilot, we add three states preceding those explicitly mentioned in the call for proposals (tested, validated exploited), namely, *initiated*, *in progress*, and *implemented*. Further, we translate the general aspects into specific feature sets of the SPARTA pilot:

- *Organisational*: roles for core pilot management, channels and repositories established to support internal reporting and the synchronization with external stakeholders.
- *Functional*: governance boards running, functional roles assigned and assumed. Established interaction patterns with external stakeholders.
- *Procedural*: processes established for single WPs, governance boards, for internal and external reporting and synchronization.
- *Operational*: established interaction models for cross-board, cross-WP, and transversal activities (roadmap, ELSA, platforms, certification), and for the pilot working as a whole.

- *Technological*: the RD&I elements of the pilot, mainly represented by the roadmap activity and SPARTA's four technical strands.

Based on this matrix of aspects and states, we assess SPARTA's achievements of the first above mentioned objective as follows:

SU-ICT-03-2020 Objective 1: Setup of a European CCN with a central competence hub						
Aspects / States	**Initiated**	**In progress**	**Implemented**	**Under Test**	**Validated**	**Exploited**
organisational	**X** (100%)	**X** (100%)	**X** (100%)	**X** (100%)	**X** (90%)	internally
functional	**X** (90%)	**X** (80%)	**X** (70%)	**X** (50%)	**X** (25%)	Internally
procedural	**X** (80%)	**X** (70%)	**X** (60%)	**X** (60%)	**X** (25%)	internally
operational	**X** (70%)	**X** (60%)	**X** (50%)	**X** (45%)	**X** (20%)	internally
technological	**X** (90%)	**X** (75%)	**X** (15%)	(?)	(?)	(?)

Table 3: SPARTA's coverage of governance aspects (estimate for Dec. 2019)

Rationale: Regarding the *organizational structure*, all elements for steering the pilot are in place. This regards the project-related and technical management (TNK/CEA) and the supporting technical infrastructure in equal terms. The validation is not yet completed with respect to the adequate utilization of the IT support structure, that is, of the optimal interplay between different notification mechanisms (individual email, mailing lists, ticket / notification / chat system), telephone- and videoconferencing, collaborative document editing system, and file repository. Some open questions still need to be addressed in future, e.g. concerning the publicly accessible WWW service, the validation level therefore is not yet 100%.

Regarding *functional* aspects, most councils, boards, task forces, directions, and working groups have been established. Still, full functional completeness has yet to be achieved, since no indicators can be provided for two out of the ten governance functions -- of the Advisory Board and the Partnership Committee (hence 80% "in process"). There is also some probability that at least one function may have to be added to address the matter of national clusters and competence centres (hence <70% implemented). Finally, the majority of transversal activities only start from the beginning of year onwards (hence, so far about 50& of the overall activities under practical test). The functions related to governance and road mapping have been tested during the first 12 months and have so far shown to be efficient and robust. For the remaining activities, similar stress tests do not exist yet, hence the relatively low validation rate of 25%.

Regarding *procedural* characteristics, the lack of indicators for activities of the Advisory Board and the Partnership Committee in conjunction with the limited activity level of the transversal activities again reduces the grades for the 'initiated" and 'in-progress' state. While the majority of processes might be defined, a good number of them are still waiting to be implemented and tested. The actual complexity of the transversal tasks has not yet become apparent, so the figures for 'implemented' and 'under test' may prove too optimistic.

Unlike the three aspects discussed so far, the level of *operational* achievements is much more difficult to gauge. This aspect concerns the operation of the pilot as a whole, so the assessment has to reflect how well pilot governance addresses the dependencies between tasks, activities, and work packages, the efficiency of dealing with and reacting to external requests, and the applicability of operational details to an institutionalized CCN instance. We have so far been unsuccessful to determine indicators that can convincingly be combined into a metric for operational readiness. This is an issue for future joint investigation with partners INOV and ISCOM.

For lack of better indicators, we arrive at our figures by translating two main qualitative factors into a quantitative assessment. First, many horizontal activities (that is, tasks with high levels of mutual dependency) were in preparatory or early stages during the first work period. Second, the roles and scopes for the envisaged ECCC and NCCs are still undecided. However, once this situation changes, mid-term adjustments to the organization, functions, and processes are likely to be

required, with possible, if temporary, negative effects on the operational efficiency of the pilot. Our conservative estimate is that the pilot runs at about two thirds of the efficiency it is likely to reach towards the end of the project. Work on about 70% of its final operational features has since been initiated. About 60% of them have been or still are under active development, and about half may have been implemented to a point where they are tested in operational practice. By now, an estimated 20% of the features may have reached a quasi-final, validated stage.

The figures on the current technological state of the pilot are based on the consideration that the four technical programs needed some ramp-up time in year one. The efficiency of the development process tends to improve substantially after an initial period, while the end of a development cycle is characterized by smoothing rough edges, documenting results, and working on end-user preferences that typically have limited implications for the underlying mechanisms. We therefore estimate that about 25% of the technical work will [11]have been carried out during the period under assessment, with an estimated 40% in year two and the remaining 35% to be addressed in year three. Work on most of the technical elements has at least been initiated (we estimate 90%) and a substantial percentage (we estimate 75%) should be work in the progress by now. However, full implementations will be the exception rather than the rule (we estimate 15%), and none of them should be expected to be in a state that would allow thorough testing.

These estimates should be revisited as soon as better figures become available from SPARTA deliverables, notably the project reports for 2019 and the information on KPIs for the technical work packages. These documents were not available when writing this report. The reader of this document is encouraged to validate the tentative statements and estimates in this section against the corresponding M12 deliverables and the feedback of the first project review.

*We conclude that SPARTA has partially achieved **objective 1**. The set-up of the governance structure, its functions, processes and supportive technology is mostly complete and under test. Due to the uncertainties about the organizational structure of cybersecurity competence centres at European level, full validation or exploitation of the governance model cannot be achieved at this stage. Judging the current operational efficiency of SPARTA's governance has therefore to be based on the achievement levels for the pilot-specific KPIs.*

2. To what extent did SPARTA contribute and strengthen cybersecurity capacities across the EU?

In SPARTA, 44 leading European institutions in cybersecurity contribute to a CCN pilot effort. More than 150 specialists from 14 European countries jointly pursue a co-ordinated research agenda. Numerous results were published in 2019 or presented at conferences and industry fairs. Since its kick-off, the pilot has co-opted some 60 organizations as associates.

Seen from this angle, the answer to the above question has to be affirmative. Intermediate results of the pilot have not yet translated into policy recommendations or adoption of technology, which is natural given the relatively early stage of the pilot. Due to the same reason, we are not yet able to offer a quantitative assessment of SPARTA's contributions to building and strengthening cybersecurity capacities across the EU in terms of economic figures. Instead, achievements and

*We conclude that by virtue of SPARTA's governance design, its technical and non-technical activities and activities, the pilot has covered **objective 2** in full.*

[11] E.g., a decision for favouring strong NCCCs with a weak ECCC hub may require to restructure the topical technical WPs (4-) as national clusters that model the executive structure of particular EU countries. This would require organizational rearrangements and potential re-allocation of resources not dedicated to technical work towards an investigation of legal and organizational requirements at national level.

impacts have to be gleaned from the progress and dissemination reports for 2019. These reports were not available when this report was produced, but preliminary information suggests that most, if not all, KPI-defined targets have been met. Again, the reader is encouraged to verify this statement against the M12 deliverables.

3. To what extent did SPARTA provide input for the future set-up of the Cybersecurity? Competence Network with a European Cybersecurity Research and Competence Centre?

It has been mentioned already that the members of the European Union have yet to reach an agreement about the operational design of a future European Cyber Competence Centre and its mode of interaction with national entities. The technical lead of SPARTA has honoured numerous requests by the EC to share his views on the state and evolution of the technical landscape in cyber security, on topics to be addressed in future, on the synchronization and orchestration between the four CCN pilots, and on the possible role, scope and operating model of future national cyber competence centres. However, *any attempt to assess, with some degree of certainty, the extent to which the input provided by SPARTA might have influenced the decision-making process of the EC and the European member states, would amount to little more than guesswork.*

Regarding the chosen organizational structure for the pilot, SPARTA's first principles laid down in Appendix X of The SPARTA DoA part B translate into

- enabling as many European players as possible to pool efforts and resources to globally compete on an equal footing,
- pursuing an inclusive strategy, working with contributors from the full range of society, industry and institutions,
- taking specific interest in questions of governance, with an emphasis on the diversity of actors and open leadership,
- favouring an institutionalized approach which maintains a maximum degree of influence, autonomy, and flexibility for the national counterparts while coordinating and steering research at European CCN level,
- contributing to raise the level of European strategic digital autonomy, and
- embracing Open Source oriented initiatives as instrumental for a future European cyber security strategy.

It cannot be precluded that a future political compromise on the role of an ECCC will settle on the smallest common denominator conceivable, i.e. on an institutional setup primarily or exclusively supporting well established, trans-European networks of dedicated national administrations (those for policing and defence come to mind here). In this case, EU funded research would be tailored to their needs, funding would be passed on to national third parties by way of cascading grant agreements. Should a settlement of this type be reached, a number of SPARTA's working hypotheses might have to be revisited.

*We conclude that SPARTA's governance has addressed **objective 3** in full, that is, to the extent that was possible under the conditions of this working period, and to the best of its abilities.*

Summary: General Objectives[12] of SU-ICT-20018-03 as Assessment Monitoring Indicators

Objective (1) is included as a RAMA candidate, i.e., for regular monitoring. Objective (2) can be ignored in future as it has been fully achieved by the formation and continued operation of the consortium. The actual achievement of Objective (3) can only be judged towards the end of the project. In the meantime, progress can be tracked based on intermediate achievements, as documented by milestones and KPIs. As this is already done in the context of WP13's project

[12] I.e., the three main objectives listed at the beginning of this part.

management, there is no need to include objective 3 as an assessment aspect for governance to be monitored on a regular basis.

Part 3: Tasks of SU-ICT-03-2018

To what extent did the structure, processes and actions of SPARTA's governance support specific tasks and aspects of the call?

To address this question, we compiled a comprehensive list of all single aspects and tasks spelled out by the SU-ICT-03-2018 call. The result can be found in Table 5. Aspects are listed in their order of appearance in the original document. Compound tasks were split into multiple single items. Some of the original wording was adjusted for reasons of grammar and intelligibility. Further, tasks (respectively *governance aspects*) have been grouped into thematic categories with a corresponding colour coding (see Table 4).

	Generic
	Technology and Innovation
	Cybersecurity Competence Network
	Demonstrator
	Assessment

Table 4: Colour coding of assessment aspects

Note: Column 2 ("M") of Table 5 flags that this assessment aspect is covered by a milestone or a KPI of the DoA. This also applies to Table 12 and Table 24.

Next, the aspects with the same theme are listed as groups. Within each such group, we determine, for each of these aspects, whether it

- Has been addressed by the DoA already (e.g. by applying certain selection criteria);
- Is applicable for this working period (M01-M12) or for later ones
- Has been fully or partially addressed during this working period or not at all;
- Is a one-time characteristic (SAMA) or an aspect that should be monitored on a regular basis (RAMA, e.g., for management controlling purposes or for being reported on in the next year's assessment -- these are marked with "Update").

In the tables for the thematic groups, the field "Nr" refers to the corresponding field in Table 5. The field "Pri" assigns a governance priority value between 0 (lowest) to 3 (highest) to the respective tasks. Here, "0" corresponds to purely optional tasks. A "1" flags tasks that should be considered, but are not mandatory, those that are self-evident by-produces, or those have been addressed by the design of the DoA already. A "2" to tasks that have partially been addressed by the DoA already, but need supplementary work or updates. Finally, "3" marks core tasks with results to be produced from scratch.

List of single tasks for a CCN pilot (from SU-ICT-2018)		
Nr	**M**	**Task / Assessment Aspect**
1		Perform common RD&I in next generation industrial and civilian cybersecurity technologies applications and services
2		Common RD&I may include dual-use cybersecurity technologies, applications and services;
3		Research on horizontal cybersecurity technologies
4		Research on cybersecurity in critical sectors (e.g. energy, transport, health, finance, eGovernment, telecom, space, manufacturing
5		Strengthen cybersecurity capacities across the EU and close the cyber skills gap
6	X	Support certification authorities with testing and validation labs equipped with state of the art technologies and expertise
7		Scale up existing competences and demonstrated strengths to the European level
8		Adopt relevant active digital ecosystems and public-private cooperation models
9		Solve technological and industrial challenges
10	X	Contribute to collectively developing and implementing a Cybersecurity Roadmap
11		Use the cPPP Strategic Research and Innovation Agenda on cyber security as a starting point
12	X	Consider the relevant work of ENISA, Europol and other EU agencies and bodies in the creation of the roadmap and its execution.
13		Set up a functional network of centres of expertise with a coordinating "competence centre"
14		Assess various organisational and legal solutions for the Cybersecurity Competence Network, taking into account various criteria (notably 14.1, 14.2, 14.3):
14.1		When assessing organisational and legal solutions for the Cybersecurity Competence Network, take into account the EU mechanisms and rules.
14.2		When assessing organisational and legal solutions for the Cybersecurity Competence Network, take into account national and regional funding structures.
14.3		When assessing organisational and legal solutions for the Cybersecurity Competence Network, also take into account funding structures offered by industry.
15		Based on the above work, a governance structure should be proposed (i.e. business model, operational and decision-making procedures/processes, technologies and people)
16	X	Governance structure, business model, operational and decision-making procedures/processes, technologies and people will be implemented, tested and validated in at least 4 demonstration cases involving all partners in the network.
17	X	The demonstrators showcase the performance of the suggested governance structure, business model, operational and decision making procedures/processes, technologies and people and their optimization (in a measurable manner).
18		Define clear milestones for the implementation of roadmap-related targets achievable by the end of the project
19		The effectiveness of the selected pilot governance structure is demonstrated by providing collaborative solutions to enhance cybersecurity capacities of the network
20		Define priorities (based on roadmap) to be addressed in the future by the Cybersecurity Competence Network.
21		The effectiveness of the selected pilot governance structure is demonstrated by by developing cyber skills (e.g. by looking at models to align cybersecurity curricula at graduate/post graduate levels; align cybersecurity certification programmes; classify skills with work roles).
22	X	Ensure outreach, raise knowledge and awareness of cybersecurity issues among a wider circle of professionals, where possible in cooperation with EU and national efforts, spread the developed expertise.
23.1	X	Together with industrial partners and their cybersecurity research collaborators, jointly identify and analyse scalable (short/mid/long term[3]) cybersecurity industrial challenges in the selected sectors
23.2		Together with industrial partners and their cybersecurity research collaborators, demonstrate their ability to collaborate in developing appropriate solutions to solve critical challenges through (not less than four) research and innovation demonstration cases

Table 5: List of all tasks from SU-ICT-03-2018

Assessment of tasks by category

Governance Tasks -- Generic				
Nr	**Pri**	**Task / Assessment Aspect**	**Evidence / Indicators**	**Coverage**
1	1	Perform common RD&I in next generation industrial and civilian cybersecurity technologies, applications and services	Co-operative process of defining RD&I goals for technology, applications and services with participation of all research institutions, industry partners, and specialized entities of national public administration. The four technical programs are up and running.	Full (for 2019)
5	1	Strengthen cybersecurity capacities across the EU and close the cyber skills gap	44 leading European institutions in cybersecurity, more than 150 specialists from 14 European, co-ordinated agenda with master theses and PhDs produced in its context, plus dedicated WP on training.	Full (update)
7	1	Scale up existing competences and demonstrated strengths to the European level		
9	1	Solve technological and industrial challenges	Four technical programs were designed in regard of specific challenges within the respective area of research and co-defined by industry. The first round of solution and approaches is presented in M12	Full (for 2019)
10	3	Contribute to collective development and implement a Cybersecurity Roadmap	The first version of the roadmap was produced in 2019, an updated one is under development	Full (for 2019) (update)
18	1	Clear milestones defined for the implementation of roadmap-related targets achievable by the end of the project	Roadmap related targets are integral parts of MS1-MS6. MS1 and MS2 are scheduled for M6 and M12. MS1 has been fully achieved, and according to preliminary information, MS2 will be as well.	Full (for 2019)
20	2	Defined priorities (based on roadmap) to be addressed in the future by the Cybersecurity Competence Network	Not applicable for the first two working periods; this is a task scheduled for the end of SPARTA's lifetime.	n/a (update) (2021)
22	2	Ensure outreach, raise knowledge and awareness of cybersecurity issues among a wider circle of professionals, **where possible in cooperation with EU and national efforts**, spread the developed expertise.	Assigned to DoA task 8.3 Synchronization events with other CCN pilots, participation at C4U event in Toulouse. Details in D1.1 (governance) and D12.3 (dissemination and communication).	Full (for 2019) (update)

Table 6: List of generic Governance Tasks

Generic governance tasks are listed in Table 6. All the aspects are fully covered. The assessment of (18) and (22) is based on preliminary information that should be validated once the corresponding reports become available.

The following aspects have been addressed by the SPARTA project design or are addressed by current activities. For the remainder of the project, they can be considered as "done":

- (1) Ongoing effort of technical programs for the full duration of the project,
- (9) Ongoing effort of technical programs for the full duration of the project,
- (18) Planning aspect, reflected by DoA

Aspects (5), (10) and (22) should be included as RAMAs and subjected to regular monitoring. The corresponding indicators all have a ternary metrics (none/partially/fully). The same applies to aspect (20), which is only relevant for the third work period.

Governance Tasks -- Technology and Innovation				
Nr	**Pri**	**Task / Assessment Aspect**	**Evidence / Indicators**	**Coverage**
2	0	Common RD&I may include dual-use cybersecurity technologies, applications and services.	Instances of dual use technologies would be escalated to the Ethics Committee. For the work period, no such instances have been reported.	Full (update)
3	3	Research on horizontal cybersecurity technologies	Horizontal cybersecurity technologies are on of the main focal points of the SPARTA cybersecurity and innovation roadmap (DoA Part B, 2.1.2.2).	Full
6	2	Support certification authorities with testing and validation labs equipped with state of the art technologies and expertise.	State of the art technologies for testing, validation and certification is specifically researched by WP5 (CAPE program), while WP11 and the Certification Task Force, and the Certification officer are tasked with the coordination of efforts and transfer of technology and methods. We are not aware that any such transfers have occurred as of December 2019.	Partial (Nascent) (update) (room for improvement)
12	1	Consider the relevant work of ENISA, Europol and other EU agencies and bodies in the creation of the roadmap and the execution.	Governance activities for structuring the work on technical solutions employed the recent JRC/ENISA taxonomy for cyber security. The state of the discussion on CCNs between the political and executive bodies of the EU and the national states is monitored, and there are ongoing efforts to synchronize with the other CCNs and ECSO. Other than this, no indicators were found that work of other European agencies has been taken into account so far. Relevant input could expected from EU funded RIAs and IAs on Safe Digital Societies (SU-DS-1-2018, SU-DS-2-2018, SU-DS-3-2019-2020), and on Open Source Hardware and Software (SMART 2019/0011).	Partial (update) (room for improvement)

Table 7: List of Technology related Governance Tasks

Table 7 lists the tasks that concern technology and innovation. The call gives explicit license for research on dual use technology, which typically tends to be discouraged in EC funded projects, as it tends to give rise to ethical concerns. Some members of the SPARTA's work in aerospace or defence, so the roadmap is likely to include topical aspects related to these areas. We found no evidence that SPARTA has approached European institutions such as the ESA or EDA. There are, however, a number of options to include or interface work from external entities in future.

From a governance perspective, addressing (2) is not mandatory, so this aspect is not a candidate for continued assessment monitoring. The same applies to aspect (3), which was and continues to be covered, throughout the lifetime of the project by the technical work programmes and the horizontal activities. Activities on certification (6) still have to get some traction, hence the qualification as "nascent". *This aspect will be included as an indicator, with a ternary metrics (none/partially/fully).* Given its currently immature state, it has been assigned a medium weight. *Aspect (12) will also be included as an indicator*. A better metrics than the tentative ternary one (none/partially/fully) is conceivable, e.g. by reflecting the number of actual uptakes, cooperations or liaisons with other EU funded pilots and projects.

Considerations for Governance: Matters of research on dual use technology and options of interfacing the EDA or similar organizations at national level might be a contemplated by ethics board. Consider alternative ways to further certification (other than directly supporting the testing and validation labs of certification authorities). Account for new options for liaising or co-operating with recently launched EC funded projects. Examine possible benefits of joint external initiatives with other CCN pilots.

Governance Tasks -- Cybersecurity Competence Network				
Nr		**Task / Assessment Aspect**	**Evidence / Indicators**	**Coverage**
8	3	Take up relevant active digital ecosystems and public-private cooperation models.	See SPARTA DoA Part B, p.10: the pilot builds on recognized national ecosystems (France, Italy, and Lithuania) and complementary formal, applied and social disciplines. The topics of the technical programs were defined with industrial input and have concrete results as requisites.	Full
11	2	Use the cPPP Strategic Research and Innovation Agenda on cyber security as a starting point	The topics of the technical programs are linked to the ECSO SRIA; this cPP has been taken into account when developing the DoA and first version of the roadmap	Full (update?)
13	3	Set up a functional network of centres of expertise with a coordinating "competence centre"	Pilot has been set up, is running and is managed according to the initial nub-spoke model	Full
23.1	3	Together with industrial partners and their cybersecurity research collaborators, collaboratively identify and analyse scalable (short/mid/long term[3]) cybersecurity industrial challenges in the selected sectors	Part of the road mapping activity. The roadmap produced in 2019 mainly describes the current state of research in cyber security, mainly focussing on short term challenges. Mid/long term challenges will be reflected in updated versions of the roadmap.	Partial (update)
23.2	3	Together with industrial partners and their cybersecurity research collaborators, demonstrate their ability to collaborate in developing appropriate solutions to solve critical challenges through (not less than four) research and innovation demonstration cases	See (1) RD&I goals for technology, application and services have been defined in an open process with participation of all research institutions, industry partners, and specialized entities of national public administration. they apply for all four technical programs that are up and running.	Full

Table 8: List of Network related Governance Tasks

The only aspect in Table 8 (CCNs) of interest for continued assessment monitoring is (23.1). The achievement of this task may rely on roadmap updates and technical insights evolving over time. The aspect maps to an indicator with ternary metrics (none/partial/fully).

None of the remaining aspects require continuous assessment:

- Aspect (8) has been addressed by the implementation of SPARTA's decision model that includes best practices from various ecosystems.
- Aspect (11) was addressed by the DoA by selecting the topics of the technical programs of WP4-7 and the creation of the first two versions of the roadmap.
- Aspect (13) has been addressed by launching these programs, and
- Aspect (23.1) is addressed in fully by the ongoing cooperative technical activities of these programs.

Governance Tasks -- Demonstrator				
Nr		**Task / Assessment Aspect**	**Evidence / Indicators**	**Coverage**
16	2	Governance structure, business model, operational and decision-making procedures/processes, technologies and people will be implemented, tested and validated in at least 4 demonstration cases involving all partners in the network.	The governance structure has been implemented in terms of operational and decision-making procedures/processes, technologies and people. On an overall pilot level, implementation of the business model translated into growing the group of associates and propagating SPARTA's goals and approach. The implementation of business models at per-partner scale is beyond the scope for this study. For details, please refer to the SPARTA management reports.	Partial (for 2019) (update)
17	3	The demonstrators showcase the performance of the suggested governance structure, business model, operational and decision making procedures/processes, technologies and people and their optimization (in a measurable manner).	The demonstrators are provided by the four technical programs of SPARTA. They are a work in progress, so the effectiveness and adequacy of the current governance model must be assessed at intermediate state, i.e., the progress made as of M12. Such an estimation currently has to rely on project-centric criteria from management reports for the first working period, which were not yet available when this document was written. The reader should consult the reports and the deliverables of the technical WPs 4-7 to determine whether the SPARTA demonstrators have reached the objectives for this working period in terms of their KPIs. Another project- rather than pilot-related criterion of success concerns all deliverables for the first working period being accepted[13].	Partial (for 2019) (update)
21	3	The effectiveness of the suggested pilot governance model is demonstrated by developing cyber skills (e.g. by looking at models to align cybersecurity curricula at graduate/post graduate levels; align cybersecurity certification programmes; classify skills with work roles).	Cybersecurity curricula alignment and development is a WP9 task that has no KPIs defined for year 1 and 2, hence, it is an unsuitable indicator for the first two work periods. Early information indicates that the applicable KPIs for awareness building, training, and cyber skill development for this period will be met. This aspect therefore qualifies as having been covered in full. The reader is invited to validate this qualification once the corresponding management reports become available.	Full

Table 9: List of Demonstrator related Governance Tasks

All aspects in Table 9 are relevant for being monitored in regular intervals. Aspect (17) was covered in full during this working period, with the exception of "measurability of optimization steps". Aspect (16) requires further decomposition for applying a provisional (ternary) metrics:

Governance elements applied at demonstrator level						
Nr	**Pri**	**Sub-Task / Aspect**	**Implemented**	**Tested**	**Validated**	**Optimized**
16.1	3	Structure	Fully	In progress	In progress	Partially
16.2	2	Business Model	Partially	In progress	No	No
16.3	2	Operational Processes	Partially	In progress	In progress	No
16.4	2	Decisional Processes.	Fully	In progress	In progress	No
16.5	3	Technologies	Partially	In progress	In progress	No
16.6	2	People	Fully	In progress	In progress	No

Table 10: Decomposition of demonstrator-related aspects

In Table 9, (16) is marked as complete *in view of what was practically achievable during the first working period* (four demonstrators launched and operating as technical programs, common high level governance structure implemented and operating), but partial in regard to testing and validation. The same applies to aspect (17), concerning measurable optimization (without preceding validation, we lack a baseline for judging optimization effects). Furthermore, the selection of the governance models for each programs was left to the responsible program leads. Although all programs use SPARTA's infrastructure, document repository and document structures, it cannot be excluded that relevant differences exist that influence the effectiveness of the overall governance model. It is a matter for future study to determine whether such effects exist (requiring decomposition to WP level).

[13] In this case, however, the quality and efficiency SPARTA's governance could be argued to be more than adequate, if not optimal already, and there would be little incentive to further optimize (and possibly over-optimize) the current organizational configuration. Consequently, it would prove difficult to demonstrate further optimization from then on.

Governance Assessment Tasks -- Assessment				
Nr		**Task / Assessment Aspect**	**Evidence / Indicators**	**Coverag**
14	3	Assess various organisational and legal solutions for the Cybersecurity Competence Network, taking into account various criteria:	These assessments were performed when the DoA was created, resulting in the current organizational structure for pilot governance. So far, all proposed organisational alternatives concerned the streamlining of project related procedures (not the pilot).	Full (update)
14.1	3	When assessing organisational and legal solutions for the Cybersecurity Competence Network, **take into account the EU mechanisms and rules,**	The structure and processes for governing the SPARTA CCN are geared at an integrative and participative model of open leadership. Similar to the operations of the European Parliament and the DGs, major decisions are based on extensive consultation. It remains to be seen whether SPARTA's processes are sufficiently agile for deal with short-term tasks and initiatives.	Partial
14.2	3	When assessing organisational and legal solutions for the Cybersecurity Competence Network, **take into account national and regional funding structures,**	Addressed by DoA Part B, section 2.1.4 and summary table in Annex IV. The structures for public funding may be revisited in the follow-up M24 deliverable D1.4 -- *Lessons learned from externally assessing a CCN pilot.*	n/a (for 2019) (update)
14.3c	3	When assessing organisational and legal solutions for the Cybersecurity Competence Network, also take into account **funding structures offered by industry**	Addressed by DoA Part B section 2.2.2, in summary table 9. The structures for industrial funding may be revisited in the follow-up M24 deliverable D1.4 -- *Lessons learned from externally assessing a CCN pilot*	n/a (for 2019) (update)
15	2	Based on the above work, a governance structure should be proposed (i.e. business model, operational and decision-making procedures/processes, technologies and people)	Addressed by DoA Part B section 3.2. So far, no substantial changes have been made to the organizational structure and processes defined in the DoA.	Full (for 2019) (update)

Table 11: List of Assessment related Governance Tasks

The question might be raised why (14) and (15) were not considered "generic" and added to this category, i.e. to Table 6. The reason for this: depending on the outcome of the political process, governance may require adjustment to reflect the structure, processes and operation of *national* competence centres. This may correspond with shifts in the powers to set the technical agendas, assign tasks, distribute research grants, and control the results, e.g. in regard to interoperability, IPR/licensing. For this reason, both aspect (14) and (15) should to be tracked continuously.

The assessment of (14.1) is supported by the practical application and test of SPARTA's decision-making process. It was used for selecting the topics for the technical programs (prior to the creation of the proposal) and for creating the roadmap. In both cases, the process proved adequate - tedious at times, but with positive effects on the level of stakeholdership. On the other hand, the pilot has to comply with all organizational and legal rules that apply to an EC funded project. Flexibility is further constrained by the lack of unallocated resources -- no financial incentives can be offered. Finally, it is virtually impossible to make short-term adjustments to the consortium contract, which imposes additional constraints. All this limits the options for determining whether the current reactiveness and flexibility of the governance model is sufficient for real-world demands.

Aspects (14.2) and (14.3) have been included, but only apply for the next reporting period. (14.2) may require further decomposition if both national and regional funding structures are relevant. The metrics for all monitoring aspects follows the ternary fully/partially/none scheme.

Considerations for Governance: Regarding aspect (14), we reiterate that a political compromise at EC level that favours strong roles for National Cybersecurity Competence Centres (including powers to determine research directions and national beneficiaries) at the expense of the central European one may invalidate SPARTA's organisational and legal working assumptions. It falls upon WP1 and WP2 to prepare for this from an organisational and legal point of view, to plan for contingencies, and, if dictated by circumstances, to suggest adjustments.

Part 4: Milestones and KPIs

Milestones describe general, high-level goals of the project. The same applies for the DoA defined KPIs. It will therefore be useful to determine whether they can also act as CNN-related aspects for governance assessment. They are listed in in Table 22 and Table 23 of Annex 2: Assessment aspects, KPIs and Milestones.

The results of matching assessment aspects against the DoA defined KPIs and milestones is displayed in Table 12. As for milestones, it turns out that each of the seven achievements for this period can be subsumed under a corresponding assessment aspect. Regarding KPIs, just two of these KPIs correspond to RAMAs, i.e., the set of aspects selected for assessment in regular intervals. The remaining five KPIs are covered by SAMAs, i.e., assessment aspects of static nature. While the DoA defined KPIs are geared towards quantification and the milestones towards ticking off groups of tasks, RAMAs and SAMAs are more oriented towards categories and discursive arguments. KPIs and milestones on the one hand and RAMAs/SAMAs on the other provide complementary metrics for gauging the quality of pilot governance.

The benefit of this complementarity can be exemplified with aspect (5), namely, to help strengthening cybersecurity capacities across the EU and closing the cyber skills gap, a requirement of much generality and macro-economic proportions. What could be a suitable indicator here? On may think of an increase in the number of cybersecurity practitioners or some measurable increase in productivity. However, impact on this scale is unrealistic for the majority EC funded projects, let alone during the first work period. SPARTA makes no exception here.

We observe that (5) is not adequately addressed by any single KPIs for this period. One could try to base the argument of having covered this requirement on the achievement of the following four KPIs:

- K3.2 (number of collaborations and liaisons with other projects), and
- K4.1 (ranking and number of publications)
- K3.1 and K6.3 (number of conferences exhibited, workshops and trainings organized, number of attendees and individuals addressed directly)

The counterargument would be that publications and liaisons with other research initiatives have no direct impact on improving operational cybersecurity capabilities on the ground, but may be correlated with them at best. If we follow this argument, the first mentioned two KPIs would have to be dismissed as not sufficiently indicative.

K3.2 and K6.3 are problematic as well. Their achievement as such provides insufficient evidence why European cybersecurity capabilities should indeed have been expanded. What can be granted, though, is that increased knowledge and skills tend to have positive impacts on productivity. This makes KPI 3.1 and KPI 6.3 admissible as indicators (albeit weak ones) for an achievement of (5). The metric could be amended, e.g. by counting the number of master and PhD theses produced in the context of SPARTA, or by counting the staff from lower ranks working on SPARTA as their first opportunity to get acquainted with the discipline of cybersecurity. On a more general line, it could be argued that the SPARTA research program in itself already contributes to strengthening Europe's cybersecurity capabilities. In this case, requirement (5) could be considered a SAMA already achieved.

We expected a substantial overlap of milestones and KPIs with our assessment aspects, since both the DoA and this study are based on the same the foundational documents, (EC political declarations, EU parliament considerations, H2020 Work Programme, and the DG call SU-ICT-03-2018). Our matching exercise shows that SPARTA's DoA meets the call requirements in full in that the KPIs and milestones cover each and every single objective and task of relevance from SU-ICT-03-2018.

Nr		Task / Monitoring Aspect	DoA defined KPIs	WPs	M12	M24.	M36
5	X	Strengthen cybersecurity capacities across the EU and closing the cyber skills gap	K3.1 # of SPARTA workshops organized and number of attendees; K6.3 # of directly addressed people (through participation at conferences, workshops, trainings, etc) by the awareness program		A		X
6	X	Support certification authorities with testing and validation labs equipped with state of the art technologies and expertise	K5.1 # of certification requirements covered by SPARTA technologies K5.3 # of platforms and access policies formally identified K5.4 Interoperability and possible joint usage of the labs	WP4-7 WP8 WP5,8	AX		
10	X	Contribute to collectively develop and implement a Cybersecurity Roadmap	K2.1 Quality and sustainability of the roadmap: # of surveys, of contributors, of revisions and feedback received, mappings with other initiatives, etc. K2.2 # of national and international calls aligned with SPARTA roadmap	WP3 WP3	AX		
12	X	Consider the relevant work of ENISA, Europol & EU agencies & bodies in the creation & execution of the roadmap	K2.1 (...) mappings with other initiatives	WP3	AX		
14.1	X	When assessing organisational and legal solutions for the Cybersecurity Competence Network, take into account the EU mechanisms and rules,	K1.1 Governance structure and decision-making mechanisms defined and implemented before M4 of the project K1.1 (see 16) K1.3 (see 16) K1.2 (see 16)	WP1 	AX AX (?) AX	A	
14.2	X	When assessing organisational and legal solutions for the Cybersecurity Competence Network, take into account national and regional funding structures,	**None applicable in first work period**	(?)		A	
14.3	X	When assessing organisational and legal solutions for the Cybersecurity Competence Network, also take into account funding structures offered by industry	**None applicable in first work period**	(?)		A	
16	X	Governance structure, business model, operational and decision-making procedures/processes, technologies and people will be implemented, tested and validated in at least 4 demonstration cases involving all partners in the network.	K1.1 Governance structure and decision making mechanisms defined and implemented before M4 of the project K1.3 Level of satisfaction of the network members (survey -- 1-7 on Likert scale) K1.2 # of issues about the governance escalated to the General Assembly	WP1 WP1,13 WP1	AX (?) AX		
17	X	The demonstrators showcase the performance of the suggested governance structure, business model, operational and decision making procedures/processes, technologies and people and their optimization (in a measurable manner).	K1.1 (see 16) K1.3 (see 16) K1.2 (see 16) K3.3 Percentage of women in groups and workshops *MS2.4 Governance internally assessed* *MS2.5 ELSA internally assessed*	WP1 WP1,13 WP1 WP2 CNR CNR	AX (?) AX AX AX AX		
22	X	Ensure outreach, raise knowledge and awareness of cybersecurity issues among a wider circle of professionals, where possible in cooperation with EU and national efforts, spread the developed expertise.	K3.1 # of SPARTA workshops organized and number of attendees K3.2 # of collaborations: liaisons with national, EU, and other projects K4.1 Ranking and # of publications K6.3 # of directly addressed people (through participation at conferences, workshops, trainings, etc) by the awareness program K6.4 # of indirectly addressed individuals (through advertisements, social media groups) by the awareness program K7.4 # of responsible R&I debates and # of participants	WP8,3,12 WP8 WP4-7 WP9,12 WP12 WP2	AX		
23.1	X	Together with industrial partners and their cybersecurity research collaborators, collaboratively identify and analyse scalable (short/mid/long term[3]) cybersecurity industrial challenges in the selected sectors	**None applicable in first work period**			A	

Table 12: Aspects for regular monitoring via assessment (A) and KPI (X)

For the sake of completeness and comparison, we also matched the DoA-defined KPIs and milestones against SAMAs, i.e., those assessment aspects that can be *disregarded* for regular monitoring. These mostly concern past matters (e.g., specific considerations that had to be reflected by proposal), so we can expect at least some of them to correspond to milestones for this work period. In fact, *all* milestones have corresponding assessment aspects (but only about half of the KPIs -- see Annex 2: Assessment aspects, KPIs and Milestones).

Findings from Part 3 and Part 4

By isolating criteria from the original call for proposals, we found 25 main assessment aspects. 21 of them are applicable for assessing the CCN pilot governance of this work period. With the evidence available in early January 2020, we find 16 out of 21 aspects fully covered. Coverage was found **partial** for 6 aspects, namely number 6 and 12 (technology, Table 7), 14 (assessment, Table 11), 16 and 17(demonstrator, Table 9), and 23 (CCN, Table 8**.**

- ***(6 - Technology)*** *Support certification authorities with testing and validation labs equipped with state of the art technologies and expertise.* There are plans in this direction, namely by WP5 and WP8, but no evidence for implementation during the first work period (progress reports and documentation for both WPs were not available for this report). Coverage is partial also in view of alternative strategies for advancing the idea of future, ubiquitous certification, which may not fully rely on official laboratories and authorities.
- **(*12 - Technology*)** *Consider the relevant work of ENISA, Europol and other EU agencies / bodies in the creation of the roadmap and the execution.* Work from ENISA, the JRC and ECSO are reflected in the DoA and the first two versions of the roadmap. We found no evidence that this work is reflected also reflected in the actual execution of the technical programs (again, due to the unavailability of the progress reports).
- ***(14 - Assessment)*** *Together with industrial partners and their cybersecurity research collaborators, collaboratively identify and analyse scalable (short/mid/long term[3]) cybersecurity industrial challenges in the selected sectors.* The roadmap identifies and address mid- and long term challenges, reflecting numerous national roadmaps, multiple verticals and industrial demands. Coverage is partial in that we found no identification and analysis of short-term challenges (arguably of lower importance, due to all-too-frequent updates of day-by-day priorities).
- **(*16 - Demonstrator*)** *Governance structure, business model, operational and decision-making procedures/processes, technologies and people will be implemented, tested and validated in at least 4 demonstration cases involving all partners in the network.* The governance structure described in the DoA defined structure is fully implemented. The operational, decision-making, technological and human aspects are under constant test. However, there is some probability of future adjustments. The actual validation and the selection of a suitable business models will not take place in year three, so coverage is only partial at this point.
- **(*17 - Demonstrator*)** *The demonstrators showcase the performance of the suggested governance structure, business model, operational and decision making procedures/processes, technologies and people and their optimization (in a measurable manner).* Structure and processes for SPARTA's pilot may have to be re-adjusted to reflect needs of more uniform second tier management (e.g., the detailed governance of the technical programs was meant to self-organize in a first cycle of determining optimal structures and processes of the very different agendas). Adjustments may also be required in response political decisions on the actual role and scope of national cybersecurity competence centres. Finally, no major reorganizations have taken place during the first work period, so there is only minimal evidence for optimization (change from monthly to quarterly reporting).
- ***(23 Network)*** *When assessing organisational and legal solutions for the Cybersecurity Competence Network, take into account the EU mechanisms and rules***.** These rules are embodied by the DoA. However, as pointed out before, important mechanisms and rules are still to be decided, and core premises of the current governance model may have to be

revisited. Amongst others, this may require an updated legal analysis (WP2) and organizational setup (WP1). We therefore do not yet consider the current state as the final one.

The complex structure of Objective (1) (see *Part 2: General Objectives of SU ICT-03-2018*), including the yet unresolved question about suitable quantitative indicators for its aspects, is a matter of further study.

Considerations for Governance: 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. To ensure that progress on these points can be measured, the intervals for internal assessment should be reduced, e.g. by combining internal assessment with the quarterly or bi-annual WP13 management reports. Alternatively, these four points could be included in the list of managed risks.

Short digression: assessment against anticipated risks

We briefly considered correlating our governance assessment aspects with the *critical implementation risks and mitigation* actions listed in the DoA. At first sight, this appeared to be a good idea: risk levels are updated in regular intervals; new risks are included as they appear, while outdated ones are be removed. At least in theory, this should yield a project-oriented, up-to-date list of factors that potentially threaten the success of CCN pilot as a whole. However, KPIs and milestones are structured around general objectives, while risks are defined for single work packages, supporting the project-oriented risk management of WP13.

The results of our attempt to map risks to assessment aspects are shown in Annex 3: Assessment Aspects and Managed Risks. *No correlation between the risks applying to specific aspects on the one hand and their actual level of coverage on the other could be found*. We therefore conclude that a risk-based assessment strategy is currently not feasible.

Considerations for Governance: The T1.4 metrics for achieving an objective and the metrics for estimating the risk of not achieving it are very loosely coupled, if coupled 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.

Summary of Parts 3 and 4

Aspects 6, 14, 16, 17, and 23 all concern work in progress, which implies just partial coverage. We attribute the partial coverage of (12) to a governance strategy of not committing to interactions with external parties during the early phases of the pilot. All other aspects have been covered in full.

On this basis, we conclude that the governance of SPARTA has achieved all tasks that could be completed during this work period. It has fully covered the general objective of implementing, testing, validating and exploiting the organisational, functional, procedural, technological and operational setup of a cybersecurity competence network with a central competence hub within the range possibilities that were available and feasible during the first assessment period.

Part 5: Potentials of the Technical Programs

Rightly or wrongly, the technical programs are considered the "core" of the CCN-projects -- see SU-ICT-03-2013 [5] where they are referred to as "demonstration cases". From the perspective of pilot governance, the technical programs are prerequisites for enabling research across topics, scientific disciplines, and projects. They also guide and enable horizontal activities such as training or outreach to the technical community and to the wider public.

All demonstrators are expected to perform cutting-edge research. In regard to the specific area of technology they are focussing on, it is of interest for governance whether these

1. match the actual scientific and technological capabilities of the project partners;
2. enable or support horizontal and outwards-facing activities;
3. permit cross-pollination, co-operation and synergy between the technical WPs;
4. support a diversity of options for different CCN models wrt. objectives and governance;
5. are capable of emulating the role of a national competence centre, if so required.

The first three points are covered by the DoA and specific activities for producing the proposal and ramping up the pilot. SPARTA's research agenda was determined by exploiting the "crowd intelligence" of all partners in a participative process. The DoA and the corresponding activities carried out during year one cover a baseline of horizontal and outwards directed activities as demanded by the call. Open Source related initiatives are addressed by WP6 in particular.

Concerning (4), uncertainties prevail about the set-up and the actual future role of a European ECCC and CCN. So far, SPARTA's technical WPs have kept all options open in addressing a range of (potentially contradictory) ECCC objectives currently under consideration:

Possible ECCC objectives				
Target Group	**Orientation**	**Pace**	**Mode**	**Capabilities**
Research	Problem oriented	Fast/ Medium	Proactive	capabilities for defining, programming, and overseeing a complex cyber security research agenda; (WP4-WP7);
Community	Program oriented	Medium/ Slow	Reactive	capabilities for interacting with adjacent ecosystems: validation & certification (WP5, WP6), academic (WP5, WP7) and industrial (WP6) training, policy makers (WP4), and the Open Source (WP6) and digital activist (WP7) spectrum;
Operative	Mission oriented	Fast/ Medium/ Slow/	Proactive/ Reactive	capabilities to interface CERTs, SIERTs, critical infrastructure, military (WP4) and critical verticals (WP6).

Table 13: Possible ECCC Objectives

Point (5) is of relevance since the balance of competencies between the planned European CCC and their national counterparts is a matter of some controversy. SPARTA may have to consider types of governance where major responsibilities (e.g. co-definition of research programs, selection of beneficiaries, and administration of grants) are assigned to national cybersecurity competence centres. This in turn may require to model and to emulate governance aspects of these NCCCs, starting with a clarification of their likely nature. For example, should they be conceptualized as a legal entity, an authority, a loose network of research groups or institutions? Essential as these questions are, they concern "external" factors not addressed in this study, but in the follow-up study D1.4. What we will address, however, is the question whether the set-up of SPARTA's technical WPs can support an exercise of modelling national CCCs internal nature.

Potential of Technical Programs for emulating National Cyber Competence Centres

WP4 is strongly guided by operative considerations. It led by partner L3CE who is executive part of the Lithuanian national cybersecurity strategy. A number of partners come from direct (Poland, Latvia) or indirect (Czechoslovakia, Germany) neighbours. Hence, WP4 might be in a position to

emulate the NCCC of a new EU member state, with supportive functions supplied evenly by "Old Europe" members (2 each for Germany, Spain, Italy, Luxembourg, Portugal, and one for France.

T-SHARK - WP4 Partner Distribution																			
Partner	6 - CESNET	8 - NIC	13 - UBO	16 - KEMEA	18 - EUT	19 - IND	25 - TCS	29 - CNR	31 - LEO	32 - KTU	33 - L3CE	34 - LKA	35 - MRU	36 - LIST	37 - SMILE	39 - LMT	41 - NASK	43 - INOV	44 - IST
Ctry	CZ	CZ	DE	DE	ESP	ESP	FR	ITA	ITA	LTU	LTU	LTU	LTU	LUX	LUX	LVA	POL	PT	PT
WP 4	12	8	14	8	8	18	18	9	23	8	24	18	10	9	6	12	16	18	12

Table 14: National / geographic Distribution of WP4 Partners

The picture for WP5 is less conclusive. Italy and Germany contribute 4 partners each, Greece, Spain, France and Greece 2 each, and Belgium, Lithuania, Luxemburg and Poland a single one. The technical program focuses on tools and mechanisms in support for verification and certification (with support for verticals). The Italian and German subgroups are on par both in terms of man months (65/63) and industry participation (LEO/SAP). A decision on the national CCC set-up to be modelled therefore has to rely on other criteria, e.g. the complexity of the national institutional setup, a majority preference of the WP5 members, or on the result of tossing a coin.

CAPE - WP5 Partner Distribution																		
Partner	1 - CEA	4 - CETIC	9 - FTS	11 - SAP	13 - UBO	14 - UKON	16 - KEMEA	17 - NCSR	18 - EUT	20 - TEC	23 - IMT	27 - CINI	28 - CNIT	29 - CNR	31 - LEO	35 - MRU	38 - UNILU	41 - NASK
Ctry	FR	BEL	DE	DE	DE	DE	GR	GR	ESP	ESP	FR	ITA	ITA	ITA	ITA	LTU	LUX	POL
WP5	21	18	18	24	10	21	10	18	10	16	24	14	12	16	23	10	9	8

Table 15: National / geographical Distribution of WP6 Partners

The picture of WP6 is mixed when it comes to national geographies of its contributors. One factor to consider here could be the level of resources assigned, another one the level of insight into the national institutional set-up for cybersecurity.

HAII-T - WP6 Partner Distribution															
Partner	2 - JR	5 - UNamur	7 - BUT	9 - FTS	12 - TUM	15 - UTARTU	23 - IMT	24 - INRIA	27 - CINI	28 - CNIT	32 - KTU	33 - L3CE	36 - LIST	38 - UNILU	40 - ITTI
Ctry	AUT	BEL	CZ	DE	DE	EST	FR	FR	ITA	ITA	LTU	LTU	LUX	LUX	POL
WP6	18	10	24	6	18	18	18	41	25	12	10	12	9	9	12

Table 16: National / geographical Distribution of WP6 Partners

WP7 is the smallest program, so the question of available resources might have to be addressed. Accounting for national majority and level of resources, the choice would fall on the Spanish NCCC.

SAFAIR - WP7 Partner Distribution							
Partner	1 - CEA	5 - UNamur	12 - TUM	20 - TEC	21 - VICOM	25 - TCS	40 - ITTI
Ctry	FR	BEL	DE	ESP	ESP	FR	POL
WP effort	6	10	12	14	24	18	18

Table 17: National / geographical Distribution of WP6 Partners

Considerations for Governance: For emulating the governance and operation of of National Competence Centres, it should be possible to use the technical programs as conduits. The NCCS of choice would be Lithuania (WP4), Italy resp. Germany (WP5), France (WP6) and Spain (WP7). All work packages, but WP5 and WP7 in particular, might require support from ELSA work packages to determine the respective institutional structure and relevant legal constraints.

Technical programs as instruments and multiplicators for CCN governance

We re-iterate that this governance assessment is *not* based on the progress reports of the technical programs, and that we are unconcerned with the actual level of technical achievements in WP4-WP7 (this is for the external reviewers to determine). Here, we are interested in estimating, for each work package, the resources available at task level, in typifying each task, characterizing the three most important topics, and target audience that would be most interested in the results.

All this is part of ongoing efforts towards a more systematic assessment of the technical WPs. Preliminary results are documented in Annex 6 Cheat Sheets for Technical WPs 4-7 as first, tentative steps towards a more quantitative approach. Our ambition is to interface, at some stage in future, with methods for industry-grade assessment. However, most indicators are currently of formal nature only, they do not have hard empirical equivalents.

For assessing the network potential and the social capital that might be created by each technical program, we use eight indicators, each of them within the range of (*0: low, 1: small, 2: average, 3: good; 4: excellent)*. They refer to the current structural prerequisites for fostering cross-fertilization between tasks and synergetic potentials with other (technical) WPs. They also concern the contribution to five specific horizontal activities included in SPARTA DoA: (1) advancement of certification, (2) provision of validation platforms, (3) education and training, (4) discourse on responsible and socially acceptable research, and (5) making provisions for Open Source.

The values currently reflect *potentials* (not *actuals*). In other words, the aspects chosen by us correspond to *ambitions* stated in the DoA, not to observed facts. These values will have to be revisited in the light of WP progress reports and deliverables that will become available in March 2020. However, even in this rudimentary state, and with a metrics that still has to be validated empirically, the table has its merits as it allows comparisons between the original aims of WP4-WP7. This can support pilot governance in its efforts of optimizing the potentials of the technical programs.

Potentials of Technical WPs										
Range: 0-4	**CrossTask**	**CrossWP)**	**Certific.**	**Platforms**	**ELSA**	**Verticals**	**Training**	**OSS**	**All Aspects**	**Estimated Potential**
WP4	3	2	0	1	2	1	1	**0**	10	3
WP5	2	2	3	3	0	3	0	1	14	3
WP6	1	2	1	1	0	1	0	1	7	2
WP7	2	1	1	1	1	0	0	0	6	2

Table 18: Potentials of Technical WPs

Some comments on the ratings assigned may be in order here:

- Few, if any of the methods researched by WP6 have (or will become) relevant for ubiquitous certification during the lifetime of the pilot, hence the low value assigned in this category.
- WP4 plans to enable a principled and public debate on the politics of cybersecurity between proponents from opposite sides of the cybersecurity spectrum: those interested to increase operative capabilities, and those guided by principles of transparency, civil rights and consumer protection. This courageous out-of-the-box initiative warrants an ELSA value of 2.
- The value for WP7 in the ELSA category was assigned since threats originating from biased AI are a growing concern that have caught the attention of the wider public.

Both WP4 and WP7 are therefore in a good position for intensified cooperation with the ELSA WP2.

WP5 and WP6 both have interfaces to Open Source related activities. It remains to be seen whether the standing and topical focus of those SPARTA members driving OSS oriented activities (SAP and INRIA) will suffice to excite developer and user communities. It could be advantageous to embed their activities within established OSS initiatives, e.g. on open toolchains or open hardware.

WP4 has some potential in the training category, as it organizes two practically oriented challenges with aspects of learning-on-the-job. Other than this, we found no indicators for interactions between technical WPs and the training and cybersecurity skills oriented activities of WP11.

Considerations for Governance: Five suggestions for emphasizing horizontal tasks: (1) So far, WP11 appears to be completely disconnected with the technical programs - some links should be fostered here (2) The technical work packages WP4 and WP7 address areas of ethical, social and political concern, offering an opportunity to jointly address them with WP2. ELSA related activities should be considered for both WP4 and WP4 beyond the level initially planned. (3) Find and exploit synergies between technical WPs by applying methods for infrastructure and "systems of systems" analysis developed by WP5. E.g., can WP5 results be used to analyse the technical setup of WP4 (or parts of it)? For aspects of task 11.4? (4) Consider to extend WP11 by a dedicated Open Source agenda, in support for WP5 and WP6 to engage with this spectrum. Can we find individuals within the consortium or the group of associates who can and are willing to act as champions? (5) The combination and unified treatment of safety and security concern is a rising topic. Are there opportunities here for co-operating with other CCN pilots, the aerospace industry, and providers for critical infrastructure?

Part 6: Views from the Trenches

The questionnaire included several fields for entering comments as free text, and 12 out of 38 respondents made use of this option. These textual comments were initially stripped from the original dataset to avoid undue influence on our assessment of assessment aspect coverage. For the same reason, these comments were processed (and are included) as the very last step of the overall assessment.

Given the unstructured nature of these contributions, we have split the comments into shorter topical statements. These were then categorized by "card shuffling", i.e. by co-locating statements of similar nature. The result of this exercise is presented in the form of nine thematic clusters that emerged from this process. All comments and single statements are included in this thematic overview.

Project related observations

1. **Project infrastructure** (4 comments): The variety of communication and collaboration tools causes problems for some partners. Suggestions were made to improve the existing mechanisms for task and deadline monitoring, and to rethink the current structure of the main document repository. The project handbook was positively acknowledged.
2. **Project communication** (4 comments): The variety of tools leads to a proliferation of communication channels, which negatively affects co-ordination. A suggestion was made to increase the granularity of the mailing lists for technical WPs, which are perceived as too noisy. There was one suggestion to allow two months notice time for meetings requiring physical presence. The SPARTA project handbook was positively acknowledged.

Pilot related observations

3. **Pilot technology issues** (2 comments): with view on the bottom-up approach or determining SPARTA's technical programs, questions were raised on the necessity and feasibility to integrate the various technologies produced by WP4-WP7. There is currently a lack of principles to guide the utilization of the common resources of SPARTA members, in particular the physical ones. These have to be worked out.
4. **Pilot strategy** (2 comments)**:** the unclear relation between SPARTA's current technological choices and volatility of the EC's political agenda for a CCN leads to some irritation. Possible thematic overlaps with other CCN pilots, and strategic uncertainties to address this issue gives rise to some concern.

5. **Pilot governance and organization** (5 comments)**:** There might be an insufficient separation between concerns of project-management on the one hand and pilot governance on the other, that is, long-term aspects concerning the actual shape and function of a future institutionalized CCN. It should also be clarified whether and to what degree the technology strands of the four programs are eventually meant to merge. It was pointed out that SPARTA currently does not have a consolidated view of capabilities that could be mobilized at partner or associates level: their research capacity, know-how, technologies, solutions, research agendas inside and outside SPARTA's programs, and the partner's needs for specific types of research, technologies and solution. A map or catalogue for the existing capabilities is deemed useful.
6. **Pilot governance and taking on new tasks** (3 comments)**:** This is acknowledged as a potentially desirable, but practically very difficult test case. Without contractual amendments, only small deviations will be possible. A consolidated roadmap and trusted working relations between the partners are considered prerequisites for reducing the risks of freeriding. These relations still need time to consolidate.
7. **Pilot governance communication** (5 comments)**:** More detailed background information for on the current EC position on the EU-CCN (and changes thereof) was asked for in one comment. There are concerns that SPARTA partners not involved in governance boards may be oblivious to committee activities of relevance to them. There is also a perceived lack of transparency regarding the technical programs of WP4-WP7 -- one comment characterized them as "black boxes", opaque for all who are not directly participating. To address this issue, one comment suggests to devote more time for presenting intermediate results from the technical WPs.
8. **Pilot governance and associates** (4 comments)**:** Multiple comments deplored uncertainness about the role, function of external stakeholders in general, and associates in particular. Little effort was made to involve external stakeholders more actively, which raises questions about their incentives and continued motivation to stay "on board". Engagement could be improved by means of dedicated communication initiatives and regular invitations to common workshops.

CCN related observations

9. **Objectives of a future European CCN institution** (4 comments)**:** There is general agreement on objectives such as the definition of a Cybersecurity Security Strategic Research Agenda and a corresponding roadmap, the prioritization and coordination of research in specific areas, or the synchronization of industrial and academic research requirements. One specific role concerns the safeguarding of long-term research agendas stretching out beyond programs, another one support and advice for finding the most promising funding instruments available for specific types of research in cyber security.

   However, there is no consensus on a possible operative role for CCNs. A suggestion was made to go beyond a purely research oriented perspective by systematically organizing topical challenges -- either in EU / Horizon2020 style (as covered by WP4) or by fostering DARPA style, topical competitions for funding. Just one of the four comments suggested a substantially expansion of CCN objectives towards operative capabilities such as passive or active countermeasures, vulnerability analysis, continuous threat modelling, and policy support beyond advice on research topics.

Considerations for Governance: (1) Find a clear *leitmotiv* and a lucid set of guiding principles. They should give a clear general direction for all SPARTAns, associates and the rest of the world. **(2)** Comments from the questionnaire suggest that there is a lack of understanding about the desirable and feasible level of integration between the technical results of WP4-WP7. To some degree, this also applies to the level of alignment between the four technical programs on the one hand and WP2, WP8 and WP11 on the other. **(3)** 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. **(4)** 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, trusted production chains ... (5) Develop a position on the feasibility and desirability of including operative capabilities as objectives for European CCNs. Should operative and research aspects kept separate and be assigned to different European agencies? Or should they both reside within a common ECCC / CCN institution?

Part 7: Assessment Assessed

In a way, this study turned to be an exercise of making lemonade from the lemons thrown by life. The lemons are embodied by the lack of technical and management reports for the fourth, and arguably most important, quarter of the review period. In November 2019, we realized that just a tiny fraction of these reports would be at our disposal for our assessment. Most of them were due in February 2020, just in time for the external review, but too late to be included in our study.

With hindsight, this is a planning error in the SPARTA proposal. The Doa should have foreseen a preliminary assessment for M12 and a finalized version for M14 that can properly reflect on the deliverables presented at the first review. As this timing problem also regards next year's assessment D1.4, we will ask for a DoA amendment to fix this issue. For the first assessment (D1.2, this document), this was not an option.

Had the reports for the first working period been at our disposal, we might have focused on methodology that takes its start points from SPARTA's *specific* objectives and KPIs as defined in the DoA. This would have been a perfectly legitimate approach. Contrary to our expectations, the majority of SPARTA's KPIs are primarily oriented towards measuring progress in terms of WP13 *project management*. Instead, they provide metrics for gauging the progress of the *pilot initiative*. However, information on the actual achievement of these KPIs would be available. This challenge had to be turned into an opportunity. It forced us to work from first principles, that is, to start out from the initial political declarations, the call for proposals, and the context set by COM(2018)630. Along this way, we explored the feasibility of including the following features:

1. Methods and indicators supporting continued assessments to meet the SU-ICT-2018-03 requirement of tracking the progress of governance (or the lack thereof) in a measurable way;
2. A subset of methods and indicators that can interface industry grade frameworks for monitoring and assessment, such as COBIT;
3. A subset of methods and indicators of sufficient generality for being applied and validated outside the specific context of SPARTA.

Point (3) is of potential relevance for all CCN pilots. Some of them may face hard choices in near future, given pilot governance objectives to align and optimize their specific combination of topical scope, reactivity, geo-administrative granularity, and stakeholder communities. We therefore started to think about complementary governance criteria for generalized CCN governance assessment and decision support method. As a result, point (1) above can now be addressed using KPI oriented indicators, aspect-oriented ones, or both of them in combination. In theory at least, this allows an experimental setup where the methods and dashboards developed by this study are applied to other pilots as well.

Questionnaire and survey

Not all questionnaires were returned, and one of our minor disappointments is the still incomplete coverage of the SPARTA partners. We deplore the return rate of less than 100%, but are ready to admit that the time around Christmas was far from ideal for launch a survey of this kind. We will complete that dataset in due time and update the figures. We expect internal assessment to become more efficient from now on since a defined process is place. A recent extension of SPARTA's infrastructure could have potentials for streamlining the data collection process. Alternatively, we could piggyback pilot governance questionnaires on regular reporting documents required by WP13 project management.

Adherence to SPARTA's performance management principles

The D1.2 study is an integral element of governance related tasks addressed by WP1 carried out in the context of T1.4. Consequently, its processes and methods had to be designed in accordance with the principles governing WP1's performance management. This translates into being simple, lightweight, and sufficiently flexible to allow for future extensions and adjustments. The baseline for a discussion whether this was achieved is Table 19, a list of the assessment targets, the instruments applied, and the estimated effort for addressing the corresponding tasks.

Simple: The questionnaire (see Annex 1: Governance Assessment Questionnaire 2019) included 12 sections. We have received no requests for clarification, so we may infer that all questions were easy to understand. **We conclude that the performance management principle of "simplicity" has been met, as far as interactions with the SPARTA partners are concerned.**

The methodology for the assessment is clearly structured, using six different, but complementary approaches produce a comprehensive view of CCN pilot governance. The categories and the criteria applied are explicit and have been motivated. Dead ends (risk-based assessment) and open issues (quantitative assessment of organizational fitness) have been highlighted. The main roadblock for delegating governance assessment to junior staff is the complexity of the pilot and its context as such, not the methodology (which we believe to be easily applicable). An educated judgement on many aspects of SPARTA is predicated on being thoroughly familiar with the DoA, actual progress in the work packages, and, not least, the research-political context. **We conjecture that the performance management principle of "simplicity" can at best be met partially, as far as it regards the methodology and its application.**

Lightweight: The questionnaires were distributed as official request via TNK, who also helped with some technical problems; we estimate the additional effort as 1 working day. During the initial phase of designing the questionnaire, we involved partner INOV with an estimated effort of 1 working day.

As shown in Table 19, the initial estimate of effort for a standard SPARTA partner not involved in WP1 was 0.25 working days. In reality, partners who chose to answer just the multiple-choice questions (including a minimum of supplementary textual information) could complete the questionnaire in no more than 15 minutes (internal test / estimate). Those who also provided text comments should have needed no more than twice this time. Some 30% has to be added to the total since several partners encountered unforeseen technical difficulties. The actual effort incurred by SPARTA partners therefore amounts to appx. 16 working hours (2 working days), that is, less than a quarter of what had been anticipated.

T1.4 Estimated effort for D1.2 assessment						
Topic / Activity	**Rounds**	**Involveds**	**Instrument**	**T1.4 effort**	**Effort per**	**Cumulative**
Pilot Lead	1	CEA	Questionnaire,	3	1	4
Project Leads	1	Technikon	Questionnaire	0.75	0.25	1
Governance, 2nd	2	All partners	Questionnaire	5 prep, 10 eval	0.25 (x44)	26
Assessment	1	ISI FHG staff	Meeting	5	0	5
Report	2	ISI FHG staff	Meetings	30	0	30
Quality control	2	2 partners	Review	2	0.5 (x 2)	3
Total				55.75	13.25	69

Table 19: Estimated Effort for D1.2 Assessment

The projected cumulative effort for all activities was about 3MM, which turned out to be a good approximation. The resources used by ISI were about 20% higher, but this is counterbalanced by the much-reduced effort for all other parties. Figures for ISI do *not* include the substantial effort for developing the methodology, as this is considered a one-off, upfront investment and part of ongoing research. Next year's assessment will add (and focus on) an external governance perspective; T1.4 therefore faces a similar level of methodological upfront investment in the upcoming period.

All other estimates correspond, within reasonable limits, to the reality encountered when carrying out the assessment. In summary, the effort for non-WP1 members was minimal. CEA and TNK had

to sacrifice 2 working days (cumulative, 1 day for completing up to two sets of questionnaires, 1 day for interviews). Excluding T1.4's initial work on methodical questions, the overall effort for carrying out this assessment (3 MMs) amount to some 0.2% of the resources allocated to the project as a whole (1747 MMs). **We conclude that this is in accordance with the performance management principle of "lightweight".**

Flexible: The questionnaires and playbooks for structured interviews can be easily adjusted to accommodate for changes of context, project direction, or as parts of preparing for governance interventions. **We therefore conclude the assessment also meets performance management principle of flexibility.**

What we did not achieve -- and why

The internal assessment is meant to complement a KPI-driven validation of governance, not least by addressing factors that lie beyond the horizon of evaluations focused on the "official" structure, functions, roles, and processes of an organization. But what sets the networked structure proposed for competence centres apart from the more traditional, dirigiste organizational model?

The functionality of a network and corresponding internal communication paths between its actors is not fully predicated by a superimposed structure of control and command represented by organizational hierarchies. Horizontal, mission-oriented and temporary interactions between members of different organizational entities are the norm rather than the exception. Networks also tend to create and reinforce allusive hierarchies of competency and authority, often misaligned with the organization chart and the officially endorsed power structure. Importantly, they also create social capital: professional favours bestowed on or owed to other actors in the network. By way of indirection ("friends of friends"), the sum of mutual obligation constitutes a kind of a network-internal currency that can be transferred and pooled.

Applied to the construct of a network of cyber competency centres pursued by CCN pilots, it would therefore be relevant if we could answer questions of the following type:

- Is there evidence for non-planned interactions between different WPs, tasks, individuals?
- Is the lifetime of a particular CCN pilot sufficient to foster the build-up of usable social capital? Are time constraints for certain partners increase reduce their chances of calling in favours?
- Can actors contributing to common platforms and initiatives build up transferable social capital? Or is everyone in it for him- or herself?
- What other incentives may exist for supporting transversal activities (e.g. between technical and non-technical strands of work)?
- Finally: are there suitable indicators for all of the above?

We believe that it should be possible to find answers to at least some of these questions. However, the empirical data we could gather so far is insufficient to address them. A major obstacle is that many interactions of potential interest evade observation since they rely on using personal email, telephone or messaging services, which are all subject to GDPR constraints.

We have not explored all possible sources of internal information yet, but those still untapped would require serious amounts of data mining to support social network analysis. As of January 2020, the document repository reports more than 3000 updates, which coincidentally comes close to the number of messages sent to internal mailing lists from February to September 2019. Hundreds of messages and documents also reside on the project management system *Stackfield,* introduced in October 2019, which offers advanced mechanisms for interaction and collaborative document editing, however, at the cost of reducing our options for straightforward statistical analysis. To correlate the information from all three sources would require a level of resources that are not at T1.4's disposal.

We will therefore not be in a position to use near-real-time data to identify nascent clusters of interactions and cross-pilot activities. This problem may become less pronounced as the pilot progresses. Successful initiatives will eventually announce their work in wider forums (at WP and internal mailing list level, at workshops and meetings, or through scientific publications). All these activities send out signals and leave traces that could be tracked.

Consideration for Governance: Upgrade the current 40-seat license for Stackfield to a corporate license. This enables currently unavailable statistical functions in support of the T1.4 internal pilot assessment.

Caveat: Significance of the Results for Governance of a Real-World European CCN

The lack of steering instruments such as financial incentives and the inflexibility of the contractual framework limits the pilot's options for major adjustments, be it in terms of governance, of adopting new fields of research, or of co-opting organizations that are not members of the consortium. More importantly, SPARTA's set-up as EU-funded project creates an incentive structure that cannot directly be compared with that of a future, institutionalized CCN. On the one hand, the partners have entered into a formal agreement described in the DoA and the consortium contract, which reflect the specific objectives of their own organization and motivates to work on common roadmaps and goals. Many of the partners have worked in collaborative research before, and their organizational DNA is geared towards scientific cooperation. These prerequisites do not easily translate into an institutional set-up where the ECCC does not have funds of their own, may not enter contractual relations, and must interact with national entities nominated by their respective countries that may follow particular rather than common agendas. In this regard, the set-up of SPARTA introduces a bias that may severely limit the relevance of our findings for a future real-world ECCC / CCN. This cannot be changed within the perimeters of the project.

Chapter 6 Recommendations, Lessons Learned, Outlook

Chapter 6 briefly revisits the process of the internal assessment. The various "Considerations for Governance" scattered across this document have been compiled into a list of actionable items. We commend it to the members of SPARTA's Strategic and Executive Boards. We close with some lessons we learned along the way and a short outlook on the future direction of our investigation.

During the final stages of our work, we carried out a number of experiments with metadata from the project management information system (mailing lists, SVN). Our preliminary conclusion is that access times and frequencies could supply valuable *supplementary* assessment indicators. A word of caution might be in order here: we emphasize that access and interaction frequencies will be *biased*, as they are likely to depend on the complexity and the workflow of the corresponding task and the working styles of the individuals involved. These and other aspects would have to be modelled first before metadata traces can be included in an internal assessment.

Considerations for Governance: Continued governance assessment could benefit from including data from the project management infrastructure, with a good chance to improve the quality of future internal assessments. However, the stated purpose of internal mailing lists or the document repository is to support the SPARTA partners in their work, not to act as a data source for an assessment purposes. We suggest presenting this issue to Ethics Committee.

We had to accept, eventually, that there was no political and very little scientific guidance for determining the future role, scope, and focus of a European CCN to any sufficient degree. As it seems, the objectives in the SU-ICT-2018-03 call *had* to be defined in such a way as to keep all options for governance open, as the actual objectives and the structure of a future ECCC still had to be hammered out on the political plane. This was probably done in the hope for swift political decisions: a political agreement would eventually be reached, which would then narrow down the governance alternatives a CCN pilot could realistically pursue in turn, and trigger corresponding adjustments. With hindsight, these hopes were misplaced, and the absence of reliable reference points now makes it difficult to assess whether a pilot is headed in the right direction.

In this situation, pilot governance can choose whether to be guided mainly (a) by the general and well-known review metrics for EU funded RIAs or (b) by the objectives (and the "spirit") of the specific call SU-ICT-2018-03 call. As a tendency, (a) discourages experimentation with governance models and institutional set-ups, while (b) might be poised to turn the challenge into an opportunity. Choosing option (a) may reduce the risk of failing on grounds of irresponsible project management, but risks to miss some of the pilot governance objectives[14]. When choosing option (b), these risks are reversed[15]. A middle path between (a) and (b) would ensure that all formal and technical objectives defined in the DoA are met while keeping all governance options open. This is a temporary choice of not making a definite choice. It was, and still may be, an optimal position, for CCN governance.[16] However, the time window for hedging bets is closing: at some stage, as each pilot has to carve out its distinctive niche of stakeholders, topics, and co-operations.

[14] As it runs against the spirit of SU-ICT-2018-03: the call, not only encourages a certain level of experimentation, but demands them as well. All aspects of pilot governance to be tested, validated, and optimized in a measurable manner. This objective cannot be met by keeping all aspects of governance static.

[15] By exploring governance models that may become obsolete once the EC members states reach an agreement on organization and scope.

[16] This is of particular for SPARTA since its governance model is tailored towards proactive, medium to long-term reactivity and participative research with contributors from the full range of society, including industry and institutions (see. Unless dictated by political development, governance will not be re-geared to support short term, mission-based and operative requirements.

6.1 Considerations for Pilot Governance

Main Findings	
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.
General Governance	
GC_G1	**Resources:** The average number of MMs allocated to governance for a EB or SB 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.
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.
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].
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.

Governance Models	
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)?
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.
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 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.
Horizontal Integration	
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.
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.
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?
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 are would act as champions?
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?

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?
Continuous Internal Assessment for Pilot	
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.
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?
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 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. 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_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.

Table 20: Considerations for Governance

6.2 Lessons Learned

1. The assessment of CCN pilots regards their suitability for emulating a future, real world CCN. However, in the absence of clear requirements, substantiated verdicts about the actual appropriateness of governance structures, processes and activities are not possible.
2. The size of the CCN project consortia and the rules for EC funded RIAs severely limit the flexibility required for an experimental approach. Lack of standard steering instruments such as sub-contracting, short-term co-option or financial incentivizing make quick and drastic changes of direction virtually impossible.
3. A well-designed governance structure can accommodate for organizational requirements not fully taken into account at proposal stage (demonstrated by the pragmatic separation of project- and pilot concerns between SPARTA's executive and strategic board).
4. The amount of effort spent on unforeseen, short-term management issues is always larger than expected, even if one accounts for this fact beforehand.
5. Honouring external requests comes at a price; it can deplete resources originally allocated for pilot-internal governance initiatives.
6. Running parallel EC projects with similar objectives in parallel runs the risk of giving rise to turf wars and posturing.
7. Political calls for ubiquitous certification for cybersecurity remain controversial. Research should not take sides here and investigate how to support alternatives to traditional certification schemes.
8. The current design of CCN does not account for capabilities that exist at more local level. Variants of CCN governance oriented towards a "Europe of Cyber Regions" are conceivable. This is exemplified by the French *Action Territoriale*, or the 2nd tier (*Laende*r) collaborative structure of regional CERTs, authorities for data protection, and PPPs (*UP KRITIS, Alliance for Cyber Security*) in Germany, or the *Interreg Europe CYBER* project.

The T1.4 deliverable for the next working period (D1.4) will assess SPARTA from an external perspective. This may allow us to take a stance that is slightly more speculative than was possible for this study. It may allow us to liberate the concept of CCN pilot governance, if only as a hypothetical exercise, from the shackles of EU project funding rules, prevailing political preferences, and considerations of institutional balance between national and European powers and competencies. This will allow to revisit some more basic premises of the call and to investigate path alternatives.

Chapter 7 Summary and Conclusion

This study is based on a methodological distinction between evaluating the performance of project management and assessing the suitability of pilot governance. The relevant baseline for governance assessment is provided by the declarations and considerations of the European institutions in 2017, and their translation into the SU-ICT-2018-03 call to submit proposals for a CCN pilot.

Following initial clarifications concerning terminology and scope, we first discussed the characteristics of the current research-political context that influence the design and adjustment of CCN pilot governance. We then presented the structure, functions and processes of SPARTA's governance both from in terms of its concepts and its practice.

The suitability of the governance was validated by examining the degree of coverage of all objectives and tasks from the call SU-ICT-2018-03. We focused on those objectives that had not already been addressed by the DoA and are of interest for regular future monitoring, as they are of relevance for future efforts to govern the pilot. A comprehensive list of these aspects can be found in Table 12.

With the exception of five horizontal activities that are work in progress, and whose actual achievement can only be judged towards the end of the project, we found all the assessment aspects under consideration to be covered in full. The structural, functional, and procedural features of SPARTA's governance have so far proven to be fit for purpose. This is not a statement about the technical achievements of the pilot during the first working period, though, which is a matter of the project reviewers to decide.

Our current insight into operational aspects of the pilot stems from direct experiences from the Executive Board and the Strategic Direction, the corresponding minutes, SPARTA's roadmap activities, the resulting first version of the roadmap (D3.1). A comprehensive investigation of the CCN pilot governance was not possible, since the M12 deliverables have not yet been published. Once they are available, they will be used for investigating indicators and for establishing a baseline for the actual operational efficiency.

Preliminary information from WP13 suggests that virtually all KPIs for the first year will be met, with overachievement in some areas. The D3.1 roadmap deliverable, which was presented to EC representatives in fall 2019, has received positive feedback as well as recommendations, which are reflected in the updated version.

Our assessment of SPARTA's governance quality in year one is generally positive. The project appears to be well on track with respect to its DoA defined objectives. This should allow SPARTA's pilot governance to pursue a more experimental and selective line of action, for example by addressing target groups with particular interests, by emphasizing specific technical themes accordingly, or by concentrating on a small number of national resp. regional geographies. Since options for project-internal re-allocation of resources are limited, this may require stepping up external co-operation.

Chapter 8 List of Abbreviations

Abbreviation	Translation
AMA	Assessment Monitoring Aspect
AMI	Assessment Monitoring Indicator
CCC	Cybersecurity Competence Centre
CCN	Cybersecurity Competence Network
CPPP	Contractual Public Private Partnership
DoA	Description of Actions (Project Plan)
EB	Executive Board
ECCC	European Cybersecurity Competence Centre
ECSO	European Cyber Security Organisation
EDA	European Defence Agency
ELSA	Ethical, Legal, Social Aspects
ENISA	European Network and Information Security Agency
ESA	European Space Agency
GDPR	General Data Protection Regulation
KPI	Key Performance Indicator
NCCC	National Cybersecurity Competence Centre
OSS	Open Source Software
RAMA	Regularly Assessed Monitoring Aspect
RIA	Research and Innovation Action
SAMA	Singularly Assessed Monitoring Aspect
SB / SD	Strategic Board / Strategic Direction
WP	Work Package

Chapter 9 Bibliography

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

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

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

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

[5] Considerations on COM(2018)630 - European Cybersecurity Industrial, Technology and Research Competence Centre and National Coordination Centres - Contribution to the Leaders' meeting, September 2018

[6] Reinhold, T.: Neue Cyberagentur: Spagat zwischen innerer und äußerer Sicherheit. Hamburg, 4/2019.
URL: https://ifsh.de/file/publication/Policy_Brief/19_04_Policy_Brief.pdf

[7] Common website for all four CCN pilots:
URL: https://cybercompetencenetwork.eu/

[8] Ebbers, Frank: Cybersecurity Strategies of Selected European Union Member State. Nov. 2019. Internal study from Fraunhofer ISI, available on request from frank.ebbers@isi.fraunhofer.de

[9] Biró M., Molnár B. Synergies Between the Common Criteria and Process Improvement. In: Abrahamsson P., Baddoo N., Margaria T., Messnarz R. (eds) Software Process Improvement. EuroSPI 2007. Lecture Notes in Computer Science, vol 4764. Springer, Berlin, Heidelberg, 2007

[10] Kaluvuri S.P., Bezzi M., Roudier Y. A Quantitative Analysis of Common Criteria Certification Practice. In: Eckert C., Katsikas S.K., Pernul G. (eds) Trust, Privacy, and Security in Digital Business. TrustBus 2014. Lecture Notes in Computer Science, vol 8647. Springer, Cham, 2014

[11] Leverett, E.; Clayton, R.; Anderson, R.: Standardisation and Certification of the 'Internet of Things'. May 2017. 16th Annual Workshop on the Economics of Information Security, La Jolla, CA 2017.
URL: https://www.cl.cam.ac.uk/~rja14/Papers/weis2017.pdf

[12] Sterlini, P.; Massacci, F; Kadenko, N.; Fiebig, M.; van Eeten, M.: Governance Challenges for European Cyber Security: Stakeholder Views.(Draft), May 2019.
URL: https://cybersec4europe.eu/wp-content/uploads/2019/11/Governance-Challenges-for-European-CyberSecurity-Policy_-Stakeholders-Views_V.Def_.pdf

[13] European Commission: SU-DS01-2018: Cybersecurity preparedness -cyber range, simulation and economics. Oct 27, 2017
URL: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/su-ds01-2018

[14] European Commission: SU-DS02-2018: Intelligent security and privacy management. Oct 27, 2017.
URL: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/su-ds02-2020

[15] European Commission: SU-DS03-2019-2020: Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises. Oct 27, 2017.
URL: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/su-ds03-2019-2020

[16] SPARTA Description of Actions, Part B, V1.0. Feb. 6, 2019.

[17] Transcription (excerpt) of structured in-depth interview with Augustin Lemesle, Dec 16 2019, 11:00h-12:15h, Paris.

[18] Transcription (excerpt) of structured in-depth interview with Florent Kirchner on Dec 16 2019, 16:15h-18:15h, Paris

Annex 1: Governance Assessment Questionnaire 2019

SPARTA Governance Assessment Questionnaire for 2019

Context	: SPARTA WP1 T1.4
Recipients	: SPARTA consortium members
Distributor	: Fraunhofer ISI
Due date	: Dec 23, 2019

Introductory remarks -- please read carefully:

This questionnaire is an integral element of the governance assessment for the SPARTA pilot during its year one. The assessment is a mandatory part for the first project review (D1.2). It is carried out by Fraunhofer ISI.

It should not take more than some instants to fill out the form. The deadline for the assessment is approaching fast, so *please take some minutes **now** to complete*.

Pressing the 'Confirm' button at the bottom of the page translates the form input into a *pre-formatted email*. Recipient and subject line should already been set when your email program spawns a window. *Please do not manually change or amend the anything!* Just press "Send" button in your email program -- this will transfer the content to Fraunhofer for further processing.

Note: If you received the form by email attachment, you may have to explicitly allow the execution of scripts from local files for the HTML form to work: ("Allow blocked content" in Internet Explorer/Edge, "file" marked as temporary trusted source in Firefox with NoScript, etc).

Note: When pressing "Confirm", the email window might be spawned *behind* that of the web browser -- check this first if nothing appears to be happening after confirmation.

Thanks in advance for completing the form and returning it in a timely fashion! Due Date is Dec 23, 2019.

Dec. 11, 2019
Dirk Kuhlmann, Fraunhofer ISI
(dirk.kuhlmann@isi.fraunhofer.de)

0. Preliminaries

Your name:

Your email:

Your organization:

How would you describe your *personal* role in SPARTA?
(multiple answers possible):

☐ cross-WP coodination ☐ WP coordination ☐ task coordination ☐ associates coodination ☐ tech/sci contributor

---

1. **When did your organization first get involved in SPARTA?**

○ Phase of initial conceptualization
○ Phase of actual proposal creation

Additional comment

2. **How did your organization get involved in SPARTA?**
(multiple answers possible)

☐ By request of SPARTA project lead
☐ By introduction / referral of other SPARTA partner
☐ By application

Additional comment

3. **Does your organization participate in EU-CCN pilots other than SPARTA?**

○ Yes ○ No

(If applicable) name(s) of other pilots

4. **How would you describe the role of your *organization* in SPARTA?**
(multiple answers possible)

☐ contributor / operative
☐ co-ordinator (leading a task or a WP leader with multiple partners)
☐ advisor (e.g. as member of ethical or exploitation board)
☐ executive (e.g. member of executive or strategic board)

Additional Comment:

5. **In your organization, how many individuals are contributing to SPARTA?**

6. **Have you / your organization collaborated with other SPARTA partners before, e.g. in other funded research projects, scientific co-operations etc?**

○ Yes ○ No

- *If the answer to the previous question was "Yes":*
  Please specify (up to three) previous collaborations.

Organization	Context	Year

7. **Does the achievement of your DoA-defined objectives depend critically on input from SPARTA tasks and WPs *other* than those you are participating in?**

○ not at all ○ negligibly ○ somewhat ○ considerably ○ crucially

Additional Comment:

If the answer to the previous question was "Yes":
Please specify (up to three) SPARTA consortium members outside your WPs and tasks you most critically depended on.

Organization	Context	Year

8. **Do you interact or maintain contacts with *external* SPARTA affiliates (members of the associates and partner program)?**

○ Yes ○ No

If the answer was "Yes", please name the affiliates:

9. **Is your organization's specific area of expertise reflected in activities highlighted by the SPARTA roadmap (WP3)?**

not at all negligibly somewhat considerably very much

Additional Comment:

10. **Please name (up to) three SPARTA consortium members (organization and individual) with whom you have collaborated most closely in 2019.**

Organization/Individual	Topic(s) / Task(s) / Frequency
	Frequency: less than quarterly quarterly monthly weekly more
	Frequency: less than quarterly quarterly monthly weekly more
	Frequency: less than quarterly quarterly monthly weekly more

11. **Since the launch of the SPARTA project, which of the following governance bodies have you been *interacting* with, *contributing* to or *contacted* by:**

Body	Frequency
Governance Board (WP1)	never rarely occasionally frequently continuously
Strategy Board (WP1)	never rarely occasionally frequently continuously
Roadmap Committee (WP3)	never rarely occasionally frequently continuously
Ethics Committee (WP2)	never rarely occasionally frequently continuously
Certification Task Force (WP1)	never rarely occasionally frequently continuously

Security Advisory Council (WP1)	never rarely occasionally frequently continuously
Associates Council (WP1)	never rarely occasionally frequently continuously
Dissemination Committee	never rarely occasionally frequently continuously
Training / Awareness Task Force	never rarely occasionally frequently continuously
Advisory Board (WP1)	never rarely occasionally frequently continuously

12. **General observations on SPARTA governance, project management, internal collaboration go here.**

Note that the pilot governance assessment is an *internal* feedback process. It is used for exploring options for a future, institutionalized Cyber Competence Network and is therefore fully independent of EC and SPARTA project controlling and management.

Please use this opportunity to add comments and suggestions for future enhancements in the text box! For a list of pressing matters, see the section below the text box.

Zurücksetzen

From a governance assessment perspective, your views on the following issues are of particular interest:

- What type of objectives can and should *realistically* be addressed by a future, institutionalized a Cyber Competence Network? (Some examples: agenda setting, advice for research bodies, ensuring continuity of long-term research agendas, coordination of research, compliancy assessment, providing capabilities for passive or active countermeasures, technical vulnerability analysis, partial or comprehensive threat monitoring, policy support ...)
- In regard to your preferences for suitable CCN-type objectives: do you think that the SPARTA pilot is on track to cover some or all of them? How do you judge the current level of alignment and co-ordination between the SPARTA work packages? Do you see straightforward ways to foster the networking between internal SPARTA members and external SPARTA associates? From the perspective of your organization: where do you see room for improvement?
- Should the agility and the capabilities of the SPARTA pilot be put to a practical test 'on the fly', e.g. by addressing new challenges not defined by the DoA, but arising from the SPARTA roadmap? What are the risks of such an experiment, and what might be a suitable scale and topic? Finally, would your organization be prepared to partake in an initiative of this kind -- resources provided?

SPARTA QUESTIONNAIRE DATASET 1											
DoA Number	DoA Name	MMs	no of tasks	Invited/recommeded	Primary member	other pilots	roles assumed	dependencies	ext. partner inv.	other pilots	leading WP	WP size (MM)
1	1-CEA	75.00	20	I	P		CW S	4	x		1	155
2	2-JR	19.00	7	I	P		S	4	x			
3	3-TNK	6.00	3	I	P		CW	0			13	66
4	4-CETIC	26.00	15	R			W T	1			11	41
5	5-UNAMUR	31.00	12	I			TA	3	x			
6	6-CESNET	19.00	11	R	P		T	0				
7	7-BUT	53.00	12	I	P		W	1	x		9	112
8	8-NIC	9.00	8	R	P		S	1	x	x		
9	9-FTS	26.00	10	I			T	0	x			
10	10-FHG	35.00	12	I		x	W	4			2	81
11	11-SAP	38.00	9	(I)			T S	1				
12	12-TUM	67.00	21	I	P		WT S	4	x		3	147
13	13-UBO	39.00	18	I			T S	0	x			
14	14-UKON	26.00	10	R			S	2				
15	15-UTARTU	19.00	7	I			S	2				
16	16-KEMEA	19.00	15	R			S	2	x			
17	17-NCSR	19.00	7	R			S	2				
18	18-EUT	19.00	11	I	P		T S	0				
20	20-TEC	35.00	13	I	P		T S	2	x			
22	22-ANSSI	5.00	14	I			C S	3	x			
23	23-IMT	81.00	18	I	P		W	1			5	282
24	24-INRIA	66.00	8	I	P		C	3		x		
25	25-TCS	44.00	15	(I)	P		T S	1	x	x		
26	27-CINI	78.00	18	I			W S	1	x		6	243
32	32-KTU	28.00	14	R			T	3	x			
33	33-L3CE	81.00	22	I	P		CW AS	3	x		4	251
34	34-LKA	19.00	7	R			T	2				
35	35-MRU	31.00	13	R			T	2				
36	36-LIST	19.00	10	I			S	0				
38	38-UNILU	19	11	I	P	x	T	0	x			
39	39-LMT	19	11	I			S	1				
40	40-ITTI	66	18	I			W S	0			7	108
41	41-NASK	32	14	R			AS	2				
42	42-PPBW	10	10	R		x	A	0	x			
43	43-INOV	45	15	R			W S	4			12	119
44	44-IST	12	4	R			S	1				

Table 21: SPARTA Questionnaire Dataset 1

Annex 2: Assessment aspects, KPIs and Milestones

	List of Milestones for month 01-12			
Nr	Milestone Title	WPs	Lead / Due	Means of Verification / Aspects
MS1	Successful SPARTA project start	1, 10, 11, 12, 13, 14 2, 3, 4, 5, 6 , 7, 8, 9	CEA, M01	MS1.1 Successful 1st General Assembly Meeting MS1.2 all legal requirements ready MS1.3 internal communication infrastructure set up
MS2	Successful SPARTA CCN launch	1, 10,2, 3, 8	CNR, M12	MS2.1 Governance operational MS2.2 Roadmap operational MS2.3 Partnership program operational MS2.4 Governance internally assessed MS2.5 ELSA internally assessed

Table 22: List of Milestones and Verification Criteria

Objective 1: Create networked governance for advanced cybersecurity research in Europe				
Nr	Description	WPs	M12 target	M12 achieved
1.1	Governance structure and decision-making mechanisms defined and implemented before M4 of the project	WP1	100%	
1.2	# of issues about the governance escalated to the General Assembly	*WP1*, WP13	< 3	
1.3	Level of satisfaction of the network members (survey -- 1-7 on Likert scale)	WP1	+5	
Objective 2: Define and sustain EU-wide R&D roadmap				
2.1	Quality and sustainability of the roadmap: # of surveys, of contributors, of revisions and feedback received, mappings with other initiatives, etc.	WP3	+20 contribs, +1 revisions, +1 mappings	
2.2	# of national and international calls aligned with SPARTA roadmap	WP3	+3	
Objective 3: Build sustained collaborations with academic, industrial, governmental, and community stakeholders				
3.1	# of SPARTA workshops organized and number of attendees	*WP8*, WP3, WP12	+12 with +20 attendees	
3.2	# of collaborations: liaisons with national, EU, and other projects	WP8	+5 collaborations	
3.3	Percentage of women in groups and workshops	WP2	+10%	
Objective 4: Innovate to address transformative strategic challenges				
4.1	Ranking and # of publications	WP4-7	+4 pub +1 top rank	
Objective 5: Support cybersecurity design, testing, evaluation and certification capabilities				
5.1	# of certification requirements covered by SPARTA technologies	WPs4-7	+6	
5.3	# of platforms and access policies formally identified	WP8	+10	
5.4	Interoperability and possible joint usage of the labs	WP5, WP8	+3 labs	
Objective 6: Enhance awareness and training capabilities and develop cybersecurity skills				
6.3	# of directly addressed people (through participation at conferences, workshops, trainings, etc) by the awareness program	WP9, WP12	+500	
6.4	# of indirectly addressed individuals (through advertisements, social media groups) by the awareness program	WP12	+2000	
Objective 7: Demonstrate ethical sustainability				
7.4	# of responsible research and innovation debates and # of participants	WP2	1 with +22 participants	

Table 23: SPARTA KPIs up to month12 (taken from DoA Part A,p6)

Nr		Task / Monitoring Aspect	DoA defined KPI or Milestone	Resp.	M12	M24	M36
1		Perform common RD&I in next generation industrial and civilian cybersecurity technologies applications and services	K3.2 # of collaborations: liaisons with national, EU, and other projects	WP8			
2		Common RD&I may include dual-use cybersecurity technologies, applications and services;, applications and services	*Neither surfaced at ethical board level nor as ELSA issue, n/a*				
3		Research on horizontal cybersecurity technologies	*fully covered by DoA and M01-M12 work, n/a*				
4		Research on cybersec in critical sectors (e.g. energy, transport, health, finance, eGovernment, telco, space, manufacturing	*fully covered by DoA and M01-M12 work, n/a*				
7		Scale up existing competences and demonstrated strengths to the European level	MS2.3 Partnership program operational K2.2 # of national and international calls aligned with SPARTA roadmap K3.2 # of collaborations: liaisons with national, EU, and other projects	WP3	X 0 0		
8		Take up relevant active digital ecosystems and public-private cooperation models	K1.1 Governance structure and decision-making mechanisms defined and implemented before M4 of the project	WP1			
9		Solve technological and industrial challenges	**To be confirmed or disputed at EC review in Feb. 2020.**				
11		Use cPPP Strategic Research / Innovation Agenda on cybersec as a starting point	MS2.2 Roadmap operational **past activity**	CNR			
13		Set up a functional network of centres of expertise with a coordinating "competence centre"	MS1.1 1st General Assembly Meeting MS1.2 all legal requirements ready MS1.3 internal communication infrastructure set up K1.1 Governance structure and decision-making mechanisms defined / implemented	CEA CEA CEA WP1			
14		Assess various organisational and legal solutions for the Cybersecurity Competence Network, taking into account various criteria:	K1.1 Governance structure and decision-making mechanisms defined and implemented before M4 of the project K1.3 Level of satisfaction of the network members (survey -- 1-7 on Likert scale) K1.2 # of issues about the governance escalated to the General Assembly	WP1 1 WP1, 1,13			
15		Based on the above work, a governance structure should be proposed (i.e. business model, operational and decision-making procedures/processes, technologies and people)	K1.1 Governance structure and decision-making mechanisms defined and implemented before M4 of the project MS2.1 Governance operational **Past activity**	WP1			
18		Clear milestones defined for the implementation of roadmap-related targets achievable by the end of the project	MS2.2 Roadmap operational **Past activity**	CNR			
19		The effectiveness of selected pilot governance structure is demonstrated by providing collaborative solutions to enhance cybersecurity capacities of the network	*For this aspect, no KPIs or Milestones defined for the first work period. T1.4 assessment relies on progress reports not available before late February 2020; it will be postponed until documentation becomes available.*				AX
20		Defined priorities (based on roadmap) to be addressed in the future by the Cybersecurity Competence Network.	MS2.2 Roadmap operational **Future activity**	CNR			AX
21		The effectiveness of selected pilot governance structure is demonstrated by by developing cyber skills (e.g. by looking at models to align cybersecurity curricula at graduate/post graduate levels; align cybersecurity certification programmes; classify skills with work roles).	*See (19).*		A		
23.2		Together with industrial partners and their cybersecurity research collaborators, demonstrate their ability to collaborate in developing appropriate solutions to solve critical challenges through (not less than four) research and innovation demonstration cases	*To be confirmed or refuted at EC review in Feb. 2020. DoA based indicators:* *MS2.4 Governance assessment* *MS2.5 ELSA assessment*		AX		

Table 24: Aspects for single assessment

For sake of completeness and comparison, we also attempted to match the DoA-defined KPIs and milestones for the first working period against assessment aspects that were *disregarded* for continuous monitoring. They mostly concern matters that lie in the past (such as details requested that had to be addressed by proposal). We can therefore expect that many of them correspond to milestones. This is indeed the case: all milestones correspond to assessment aspects, but about half of the KPIs do not -- see table below.

KPI	Description
2.1	Quality and sustainability of the roadmap: # of surveys, contributors, revisions and feedback received, mappings with other
2.2	# of national and international calls aligned with SPARTA roadmap
3.3	Percentage of women in groups and workshops
4.1	Ranking and # of publications
5.1	# of certification requirements covered by SPARTA technologies
5.2	# of platforms and access policies formally identified
6.4	# of indirectly addressed individuals (through advertisements, social media groups) by the awareness program
7.4	# of responsible R&I debates and # of participants

Table 25: KPIs not corresponding to any static assessment aspect.

The takeaway of this comparison is that assessments based on continuously monitored aspects from Table 12 always allow assuming either a pilot-oriented or a project-oriented perspective.

Annex 3: Assessment Aspects and Managed Risks

We were interested whether the type and level of managed risks can be used as a signal for the coverage of specific assessment aspects. The underlying idea was that aspects more exposed to risk might have a smaller probability of achieving full coverage. We disclose right from the start that no correlation between currently managed risks and aspect coverage could be found. Risk management in its current form offers no support for substantiating coverage statements. A brief description of the approach we took is documented in this annex for sake of completeness only. It adds nothing to the actual findings of the assessment, so the reader should feel free to skip it.

The set of risks that may affect assessment aspects for pilot governance is retrieved from the list *WT5 Critical Implementation risks and mitigation (*SPARTA DoA Part A, section 1.3.5). We are mainly concerned with the set of risks relating to the governance and the horizontal activities of the pilot. An exception from this rule are risks related to integration, since they affect the pilot as a whole. The corresponding subset (referred to as GRR -- governance relevant risks) is shown in Table 26.

Managed risks correspond to work packages, not to pilot objectives. We therefore equip each risk from the GRR subset by a list of aspects (pilot level tasks) it may affect. As can be seen from the rightmost column of Table 27, risks can be relevant for as many as five assessment aspects simultaneously. The table also includes our attempt to chunk the various mitigation strategies into single-action items.

A particular risk may affect different aspects to different degrees, which we reflect by introducing a weight factor, a discrete value from the set {1,2,3}). Weights were assigned by estimating whether the impact of the substantiated risk would be benign (1), confined to partial activities / single work packages (2) , or have repercussions beyond this (3), We mapped the ternary "low", "medium", and "high" metrics for risk severity correspondingly to the discrete values of 1, 2 and 3. By multiplying weights and the numeric representation of the risk levels, we obtain the weighted risk value WR. Finally, we calculate the cumulative weighted risk (CWR) for each assessment aspect by adding up the WRs for all risks affecting it. The results are shown in the rightmost column of Table 28.

A compressed version of it, with rows sorted in descending CWR order, is shown in Table 29. The reader may convince herself that the risk exposure and level of coverage appear to be unrelated. Should there be a deeper pattern, we are unlikely to find it, as at most two follow-up assessments will be carried out over the duration of SPARTA. We conclude that data from project risk management in its current form currently is of no practical value for our purposes and abandon this line of investigation.

List of Managed Risks of Relevance for Pilot Governance				
Risk number	**Description of Risk**	**Risk (L/M/H)**	**WP #**	**Proposed risk mitigation**
2	Governance audits provide recommendations too expensive to be implemented with the current budget	Medium	WP1	Cost and impact of recommendations will be estimated to allow their prioritization.
4	Lack of cooperation of SPARTA Programs	Low	WP2	Involvement of WP3-WP6 leads in WP2 focusing on ethical, legal and societal aspects
8	Lack of focus and / or funding	Medium	WP3	Due to the requirement to build a comprehensive European roadmap this risk is likely to occur and can only be mitigated by extensive funding. Nevertheless, only selected Programs are implemented within the SPARTA context and the roadmap contents are continuously reviewed and readjusted in T3.5
9	Challenge will end up with no concrete result	Medium	WP4	Timely reviews will be assured. The methodology foresees phases based execution to verify midterm results in early stages.
11	Resources allocated for each challenge will be insufficient to execute the whole challenge	High	WP4	The Program Lead will perform an assessment of do-ability based on the resources allocated for each challenge execution.
14	**Integration** of tools on demonstrators	Medium	WP5	The specification of the demonstrators is addressed early in WP4 and is closely linked to the development of tools, in order to limit integration risk. Tool status with respect to demonstrators will be reviewed every 3 months starting M12.
17	Failure to achieve effective **integration**	Medium	WP6	Integration requirements will be defined in the early stages and prototypes will be assessed against integration requirements on a regular basis
21	Difficulties in validation at use-cases and verticals	High	WP7	Consortium will leverage the Associates Council, work on early contacts with end-users on potential use-cases, and will work on representative laboratory evaluations and testing on relevant and realistic data.
22	Lack of **integration** among the platforms	Medium	WP8	The possible integration strategies have been analysed during proposal preparation. All the partners are committed and have the necessary experience. Monitoring of the situation and possibly reshaping of the goals.
23	Lack of **integration** of national ecosystems	Low	WP8	SPARTA consortium pulled together existing national cluster where the members expressed a strong commitment to cooperation and further aggregation. The strong support of national agencies is an added value
24	Lack of **integration** at European Level	Medium	WP8	SPARTA consortium members are used to work at European level in EU projects and activities. Monitoring of the situation, promotion of the approach and possibly reshaping of the goals.
30	Cybersecurity certification initiatives evolve over project duration	Medium	WP11	SPARTA will monitor European and national cybersecurity initiatives during the entire SPARTA project, and changes will be taken into account for SPARTA activities.
33	Lack of interest and engagement from stakeholders and target audiences	Medium	WP12	Engagement and awareness will be an active part of the work done by the 44 SPARTA partners, who have an extensive outreach network that will be leveraged by WP12 to maximise impact and reduce risk.

Table 26: Relevant managed Risks for Pilot Governance (excerpt SARTA DoA Part A 1.3.5)

Critical implementation risks and affected tasks (pilot-oriented perspective)					
Risk #	**Description of Risk**	**Risk**	**WP #**	**Proposed risk mitigation**	**Risk for**
R02	Governance audit recommendations too expensive to be implemented within current budget	Med	WP1	RM02.1 Estimate cost and impact of recommendations RM02.2 Prioritize implementation of changes based on Cost / Impact considerations.	A14 A15 A17
R04	Lack of cooperation of SPARTA Programs with ELSA activities	Low	WP2	RM04.1 Involve WP3-WP6 leads in WP2 on ELSA	A7 A8 A14.1 S14.2 A17 A22
R08	Lack of focus and / or funding[17]for participating in joint roadmap efforts	Med	WP3	RM08.1 Can only be mitigated by extensive funding. RM08.2 Continuously review and readjust roadmap in T3.5	A10 A12 A18 A20 A23.1
R09	A challenge ends up with no concrete result	Med	WP4	RM09.1 Assure timely reviews of challenges vs. results RM09.2 Use methodology with phases based execution to verify midterm results in early stages.	A16 A23.2
R11	A challenge has Insufficient resources for fully executing it	High	WP4	RM11.1 For executing each challenge, Program Lead assesses do-ability within allocated resources	A16 A23.2
R14	**Integration** of tools on demonstrators	Med	WP5	RM14.1 Early specification of demonstrators RM14.2 Link demonstrator specification to development of tools RM14.3 Quarterly review tools status wrt demonstrators, starting M12.	A3 A9 A16 A19 A23.2
R17	Failure to achieve effective **integration**	Med	WP6	RM17.1 Define integration requirements in the early stages RM17.2 Regularly assess prototypes against integration requirements	A3 A9 A16 A19 A23.2
R21	Difficulties in validation for use-cases and verticals	High	WP7	RM21.1 Leverage Associates Council RM21.2 Make early contacts with end-users on potential use-cases RM21.3 Work on representative laboratory evaluations and testing on relevant and realistic data.	A1 A4 A9 A23.2
R22	Lack of **integration** among the platforms	Med	WP8	RM22.1 Monitor the situation (*intervals? escalation process?*) RM22.2 Reshape goals if so required	A3 A13 A19
R23	Lack of **integration** of national ecosystems	Low	WP8	RM23.1 Leverage existing national clusters RM23.1 Maintain existing commitment to cooperation and further aggregation. RM23.1 Ensure continued support of national agencies	A13 A15
R24	Lack of **integration** at European Level	Med	WP8	RM24.1 Monitor the situation (*Intervals? Escalation process?*) RM24.2 Promote chosen approach RM24.3 Reshape the goals if so required	A13 A15
R30	Cybersecurity certification initiatives evolve over project duration	Med	WP11	RM30.1 Monitor European and national cybersecurity initiatives RM30.2 Account for and signal implications of changes For SPARTA Activities	A6 A21
R33	Lack of interest and engagement from stakeholders and target audiences	Med	WP12	RM33.1 Leverage extensive outreach network.	A5 A22

Table 27: Assessment aspects matched against risks

[17] **Rationale:** The call SO-ICT-03-2018 appears to have been predicated on the assumption that (some) of the CCN's technical strands would be selected as a result of the roadmap exercise, and therefore assume this roadmap to be implemented (at least in parts, see assessment aspect A10). However, SPARTA selected its four technical programs occurred **prior** to the project launch, that is, also prior to the systematic development of its roadmap: in fact, the selection process for the programs can be considered as a structured, still 'unofficial' first step towards the roadmap design. The proposal evaluation acknowledged as an attempt to increase efficiency. The 'official' roadmap activities started when the project was launched. Its brief is the DoA defined objective to create a comprehensive European roadmap, which, by its nature, will by far exceed the scope of the four programs. Thusly the concern that the self-interest of the preselected programs (which are topically represented in the roadmap) could hamper efforts geared towards comprehensiveness.

Pilot Governance Relevant Aspects and corresponding Risks, Weighted and Cumulative Risks								
Nr	**M**	**Task / Assessment Aspect**	**Description of Risk**	**R**	**WP**	**W**	**WR**	**CWR**
A1		Perform common RD&I in next generation industrial and civilian cybersecurity technologies applications and services	R21 Difficulties in validation for use-cases and verticals	High	WP7	2	6	6
A2		Common RD&I may include dual-use cybersecurity technologies, applications and services,						
A3		Research on horizontal cybersecurity technologies	R14 **Integration** of tools on demonstrators R22 Lack of **integration** among the platforms	Med Med	WP5 WP8	2 3	4 6	10
A4		Research on cybersecurity in critical sectors (e.g. energy, transport, health, finance, eGovernment, telecom, space, manufacturing	R21 Difficulties in validation for use-cases and verticals	High	WP7	3	9	9
A5		Strengthen cybersecurity capacities across the EU and closing the cyber skills gap	R33 Lack of interest and engagement from stakeholders and target audiences	Med	WP12	3	6	6
A6	X	Support certification authorities with testing and validation labs equipped with state of the art technologies and expertise	R30 Cybersecurity certification initiatives evolve over project duration	Med	WP11	1	2	2
A7		Scale up existing competences and demonstrated strengths to the European level	R4 Lack of cooperation of SPARTA Programs with ELSA activities	Low	WP2	1	1	1
A8		Take up relevant active digital ecosystems and public-private cooperation models	R4 Lack of cooperation of SPARTA Programs with ELSA activities	Low	WP2	2	2	2
A9		Solve technological and industrial challenges	R09 A challenge ends up with no concrete result R11 A challenge has Insufficient resources for fully executing it R14 **Integration** of tools on demonstrators R17 Failure to achieve effective **integration**	Med High Med Med	WP4 WP4 WP5 WP6	1 1 2 2	2 3 4 4	13
A10	X	Contribute to collectively develop and implement a Cybersecurity Roadmap	R08 Lack of focus and / or funding for participating in joint roadmap efforts	Med	WP3	3	6	6
A11		Use the cPPP Strategic Research and Innovation Agenda on cyber security as a starting point						
A12	X	Consider the relevant work of ENISA, Europol and other EU agencies and bodies in the creation of the roadmap and the execution.	R08 Lack of focus and / or funding for participating in joint roadmap efforts	Med	WP3	2	4	4
A13		Set up a functional network of centres of expertise with a coordinating "competence centre"	R23 Lack of **integration** of national ecosystems R24 Lack of **integration** at European level	Low Med	WP8 WP8	2 3	2 6	10
A14		Assess various organisational and legal solutions for the Cybersecurity Competence Network, taking into account various criteria:	R01 Governance audit recommendations too expensive to be implemented within current budget	Med	WP1	2	4	4
A14.1		When assessing organisational and **legal solutions** for the Cybersecurity Competence Network, take into account **the EU mechanisms and rules**,	R04 Lack of cooperation of SPARTA Programs with ELSA activities[18]	Low	WP2	1	1	1
A14.2		When (…, see 14.1), take into account national and regional funding structures,	R04 Lack of cooperation of SPARTA Programs with ELSA activities[19]	Low	WP2	1	1	1
A14.3		When(…, see 14.1) , also take into account funding structures offered by industry	R01 Governance audit recommendations too expensive to be implemented within current budget	Med	WP1	1	2	2

[18] *Note: R04 regards possibly required legal analysis of EU mechanisms rules*

[19] *Note: R04 regards possibly required updated analysis on relevance of national funding*

Pilot Governance Relevant Aspects and corresponding Risks, Weighted and Cumulative Risks								
Nr	**M**	**Task / Assessment Aspect**	**Description of Risk**	**R**	**WP**	**W**	**WR**	**CWR**
A15		Based on the above work, a governance structure should be proposed (i.e. business model, operational and decision-making procedures/processes, technologies and people)	R01 Governance audit recommendations too expensive to be implemented within current budget	Med	WP1	1	2	8
			R23 Lack of **integration** of national ecosystems	Low	WP8	2	2	
			R24 Lack of **integration** at European level	Med	WP8	2	4	
A16	X	Governance structure, business model, operational and decision-making procedures/processes, technologies and people will be **implemented, tested and validated** in at least 4 demonstration cases involving all partners in the network.	R09 A challenge ends up with no concrete result	Med	WP4	2	4	17
			R11 A challenge has Insufficient resources for fully executing it	High	WP4	1	3	
			R14 **Integration** of tools on demonstrators	Med	WP5	2	4	
			R17 Failure to achieve effective **integration**	Med	WP6	3	6	
A17	X	The demonstrators showcase the performance of the suggested governance structure, business model, operational and decision making procedures/processes, technologies and people **and their optimization (in a measurable manner).**	R01 Governance audit recommendations too expensive to be implemented within current budget	Med	WP1	2	2	3
			R04 Lack of cooperation of SPARTA R04 Programs with ELSA activities[20]	Low	WP2	1	1	
A18		Clear milestones defined for the implementation of roadmap-related targets achievable by the end of the project	R08 Lack of focus and / or funding for participating in joint roadmap efforts	Med	WP3	3	6	6
A19		The effectiveness of selected pilot governance structure is demonstrated by providing **collaborative solutions** to enhance cybersecurity capacities of the network	R14 **Integration** of tools on demonstrators	Med	WP5	2	4	8
			R22 Lack of **integration** among the platforms	Med	WP8	2	4	
A20		Defined priorities (based on roadmap) to be addressed in the future by the Cybersecurity Competence Network.	R08 Lack of focus and / or funding for participating in joint roadmap efforts	Med	WP3	1	2	2
A21		The effectiveness of selected pilot governance structure is demonstrated by developing **cyber skills** (e.g. by looking at models to align cybersecurity curricula at graduate/post graduate levels; **align cybersecurity certification programmes**; classify skills with work roles).	R30 Cybersecurity certification initiatives evolve over project duration	Med	WP11	1	2	2
A22	X	Ensure outreach, raise knowledge and awareness of cybersecurity issues among a wider circle of professionals, where possible in cooperation with EU and national efforts, spread the developed expertise.	R04 Lack of cooperation of SPARTA Programs with ELSA activities	Low	WP2	1	1	1
			R33 Lack of interest and engagement from stakeholders and target audiences	Med	WP12	3	6	
A23.1	X	Together with industrial partners and their cybersecurity research collaborators, collaboratively identify and analyse scalable (short/mid /long term[3]) cybersecurity industrial challenges in the selected sectors	R08 Lack of focus and / or funding for participating in joint roadmap efforts	Med	WP3	2	1	2
A23.2		Together (...), demonstrate their ability to collaborate in **developing appropriate solutions to solve critical challenges** through (not less than four) research and innovation demonstration cases	R09 A challenge ends up with no concrete result	Med	WP4	2	4	12
			R11 A challenge has Insufficient resources for fully executing it	High	WP4	1	3	
			R17 Failure to achieve effective **integration**	Med	WP5	3		
			R21 Difficulties in validation for use-cases and verticals	High	WP7	2		

Table 28: Project Governance Aspects and corresponding Risks

[20] *Note: R04 concerns ELSA-guided changes of structure, processes, decision making, and business models*

Assessment Aspects sorted by Cumulative Weighted Risk (CWA, 3rd column)				
Nr	Task / Assessment Aspect	CWR	Coverage (F)ull / (P)artial)	
A16	Governance structure, business model, operational and decision-making procedures/processes, technologies and people will be **implemented, tested and validated** in at least 4 demonstration cases involving all partners in the network.	17	P	for 1st period, future / final
A9	Solve technological and industrial challenges	13	F	ongoing effort
A23.2	Together (...), demonstrate their ability to collaborate in **developing appropriate solutions to solve critical challenges** through (not less than four) research and innovation demonstration cases	12	F	for 1st period
A3	Research on horizontal cybersecurity technologies	10	F	for 1st period
A13	Set up a functional network of centres of expertise with a coordinating "competence centre"	10	F	for 1st period
A4	Research on cybersecurity in critical sectors (e.g. energy, transport, health, finance, eGovernment, telecom, space, manufacturing	9	F	for 1st period
A15	Based on the above work, a governance structure should be proposed (i.e. business model, operational and decision-making procedures/processes, technologies and people)	8	P	not yet finalized
A19	The effectiveness of selected pilot governance structure is demonstrated by providing **collaborative solutions** to enhance cybersecurity capacities of the network	8	P	not yet finalized
A1	Perform common RD&I in next generation industrial and civilian cybersecurity technologies applications and services	6	F	ongoing effort
A5	Strengthen cybersecurity capacities across the EU and closing the cyber skills gap	6	F	ongoing effort
A10	Contribute to collectively develop and implement a Cybersecurity Roadmap	6	F	for 1st period
A18	Clear milestones defined for the implementation of roadmap-related targets achievable by the end of the project	6	F	by DoA
A12	Consider the relevant work of ENISA, Europol and other EU agencies and bodies in the creation of the roadmap and the execution.	4	P	reconsider
A14	Assess various organisational and legal solutions for the Cybersecurity Competence Network, taking into account various criteria:	4	F	by DoA
A17	The demonstrators showcase the performance of the suggested governance structure, business model, operational and decision making procedures/processes, technologies and people **and their optimization (in a measurable manner).**	3	P	future / final
A6	Support certification authorities with testing and validation labs equipped with state of the art technologies and expertise	2	P	not yet finalized
A8	Take up relevant active digital ecosystems and public-private cooperation models	2	F	by DoA
A14.3	When(..., see 14.1) , also take into account funding structures offered by industry	2	n/a	future
A20	Defined priorities (based on roadmap) to be addressed in the future by the Cybersecurity Competence Network.	2	n/a	future
A21	The effectiveness of selected pilot governance structure is demonstrated by developing **cyber skills** (e.g. by looking at models to align cybersecurity curricula at graduate/post graduate levels; **align cybersecurity certification programmes**; classify skills with work roles).	2	F	for 1st period
A23.1	Together with industrial partners and their cybersecurity research collaborators, collaboratively identify and analyse scalable (short/mid/long term[3]) cybersecurity industrial challenges in the selected sectors	2	P	not yet finalized
A7	Scale up existing competences and demonstrated strengths to the European level	1	P	Unclear criteria
A14.1	When assessing organisational and **legal solutions** for the Cybersecurity Competence Network, take into account **the EU mechanisms and rules**	1	P	not finalized
A14.2	When (..., see 14.1), take into account national and regional funding structures,	1	n/a	DoA / future
A22	Ensure outreach, raise knowledge and awareness of cybersecurity issues among a wider circle of professionals, where possible in cooperation with EU and national efforts, spread the developed expertise.	1	F	for 1st period
A2	Common RD&I may include dual-use cybersecurity technologies, applications and services,		F	optional
A11	Use the cPPP Strategic Research and Innovation Agenda on cyber security as a starting point		F	by DoAI

Table 29: Pilot Governance Aspects sorted by Cumulative Weighted Risk

Annex 4: Statements from European Institutions

Note: the following quotations have been partially marked up. Grey sections highlight those objectives and tasks that constitute the basis for the assessment. Shorter sections with bold characters emphasize details of particular interest. Apart from the section headings, the original text passages include no bold characters.

President Jean-Claude Juncker
State of the Union Address.
Sep 13, 2017 [1]

*Europe is still not well equipped when it comes to cyber-attacks. Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks. Cyber-attacks know no borders and no one is immune. This is why, today, the Commission is proposing new tools**, including** a European Cybersecurity Agency, to help defend us against such attacks.*

European Commission:
State of the Union -- Cybersecurity: Commission scales up EU's response to cyber-attacks.
Sep 19, 2017. [2]

*To equip Europe with the right tools to deal with cyber-attacks, the European Commission and the High Representative are proposing a wide-ranging set of measures to build strong cybersecurity in the EU. This **includes** a proposal for an EU Cybersecurity Agency to assist Member States in dealing with cyber-attacks, as well as a new European certification scheme that will ensure that products and services in the digital world are safe to use.*

Speech by President-elect von der Leyen in the European Parliament Plenary on the occasion of the presentation of her College or Commissioners and their programme.
Nov 27, 2019. [3]

*Cyber security and digitalisation are two sides of the same coin. This is why cyber security is a top priority. For the competitiveness of European companies, we have to have stringent security requirements and a unified European approach. We have to share our knowledge of the dangers. We need a common platform; we need an **enhanced** European Cybersecurity Agency. That is the only way we can strengthen trust in the connected economy and boost resilience to dangers of all kinds.*
[...]
*An EU Cybersecurity Agency: Building on the existing European Agency for Network and Information Security (ENISA), the Agency will be given a permanent mandate to assist Member States in effectively preventing and responding to cyber-attacks. It will improve the EU's preparedness to react by organising yearly pan-European cybersecurity exercises and by ensuring better sharing of threat intelligence and knowledge through the setting up of Information Sharing and Analyses Centres. It will help implement the Directive on the Security of Network and Information Systems which contains reporting obligations **to national authorities** in case of serious incidents.*

The Cybersecurity Agency would also help put in place and implement the EU-wide certification framework that the Commission is proposing to ensure that products and services are cyber secure. Just as consumers can trust what they eat thanks to EU food labels, new European cybersecurity certificates will ensure the trustworthiness of the billions of devices ("Internet of Things") which drive today's critical infrastructures, such as energy and transport networks, but also new consumer devices, such as connected cars. Cybersecurity certificates will be recognised across Member States, thereby cutting down on the administrative burden and costs [1] for companies.

[T]he Commission and the High Representative are proposing:

- *A European Cybersecurity Research and Competence Centre (pilot to be set up in the course of 2018). Working with Member States, it **will help develop and roll out the tools and technology needed to keep up with an ever-changing threat** and [...] **will complement capacity-building** efforts in this area at EU and national level. (...)*
- *Stronger cyber defence capabilities: Member States **are encouraged** to include cyber defence within the Framework of **Permanent Structured Cooperation (PESCO) and the European Defence Fund** to support cyber defence projects. The European Cybersecurity Research and Competence Centre could also be further developed with a cyber defence dimension. To address the skills gap in cyber defence, the EU will create a cyber defence training and education platform in 2018. The EU and NATO will together foster cyber defence research and innovation cooperation. Cooperation with NATO, including participation in parallel and coordinated exercises, will be deepened.*

European Commission:
Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap.
Oct 27, 2017 [4]

Topic Description

Specific Challenge:

The Public Private Partnership on Cybersecurity[1] created in 2016 was an important first step aiming at triggering up to EUR 1.8 billion of investment. However, the scale of the investment under way in other parts of the world suggests that the EU needs to do more in terms of investment and overcome the fragmentation of capacities spread across the EU. In this context in a recent Joint Communication[2] the Commission announced the intention to create a Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre.

Scope

*The objective of this topic is to scale up existing research for the benefit of the cybersecurity of the Digital Single Market, with solutions that **can** be marketable. For this, participants should in parallel propose, test, validate and exploit the possible organisational, functional, procedural, technological and operational setup of a cybersecurity competence network with a central competence hub. Projects under this topic will (...) provide valuable input for the future set-up of the Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre as mentioned by the Joint Communication.*

To achieve the above, support will go to consortia of competence centres in cybersecurity to engage together in:

- *Common research, development and innovation in next generation industrial and civilian cybersecurity technologies (including dual-use), applications and services; focus should be on horizontal cybersecurity technologies as well as on cybersecurity in critical sectors (e.g. energy, transport, health, finance, eGovernment, telecom, space, manufacturing);*
- *Strengthening cybersecurity capacities across the EU and closing the cyber skills gap;*
- *Supporting certification authorities with testing and validation labs equipped with state of the art technologies and expertise.*

*Each proposal should bring together cybersecurity R&D&I centres in Europe (e.g. university labs/public or private non-profit research centres) to create synergies and scale up existing competences and demonstrated strengths to the European level. (...) When developing the Roadmap, the results of the work done by the cPPP on cybersecurity, notably its Strategic Research and Innovation Agenda, will serve as a starting point. **Consideration should also be given to the relevant work of ENISA, Europol and other EU agencies and bodies.***

To implement this Roadmap, partners in the proposal(s) are expected to set up a functional network of centres of expertise with a coordinating "competence centre" (this role should be undertaken by one of the partners in the network, with the necessary capacity, resources and experience). Work includes the assessment of various organisational and legal solutions for the

Cybersecurity Competence Network, taking into account various criteria, including the EU mechanisms and rules, ***national and regional funding structures****, as well as those offered by industry. Based on the above work,* ***a governance structure should be proposed*** *(i.e. business model, operational and decision-making procedures/processes, technologies and people) and will be implemented, tested and validated in the demonstration cases (see below) involving all partners in the network to showcase (in a measurable manner) its performance and optimise the suggested governance structure.*

Projects will demonstrate the effectiveness of their selected governance structure by ***providing collaborative solutions*** *to enhance cybersecurity capacities of the network and develop cyber skills (e.g. by looking at models to align cybersecurity curricula at graduate/post graduate levels;* ***align cybersecurity certification programmes; classify skills with work roles).***

Projects should ensure outreach, to raise knowledge and awareness of cybersecurity issues among a wider circle of professionals, ***where possible in cooperation with EU and national efforts****, and to spread the developed expertise.*

Projects should also include industrial partners and their cybersecurity research collaborators to create synergies and: (a) collaboratively ***identify and analyse scalable (short/mid/long term[3]) cybersecurity industrial challenges*** *in the selected sectors and (b) demonstrate their ability to collaborate in developing appropriate solutions to solve critical challenges through (not less than four) research and innovation demonstration cases.*

These demonstration cases will constitute the core part of the work to be done within the project. They will be based on a specific research & development roadmap to tackle selected industrial challenges and will implement it covering a complete range of activities, from research & innovation through testing, experimentation and validation to certification activities.

Projects under this topic are implemented as a programme through the use of complementary grants. The respective options of Article 2, Article 31.6 and Article 41.4 of the Model Grant Agreement will be applied. Proposals shall therefore foresee resources for clustering activities with other projects funded under this topic to identify synergies, best practices and kick-off the process of creating the network involving the sub-networks already created by awarded projects. This task will contribute to the actual set-up of the Cybersecurity Competence Network and a European Cybersecurity Research and Competence Centre at a later stage.

*A proposal must involve distinct cybersecurity R&D&I excellence centres in Europe (e.g. university labs, public or private non-profit research centres, taking into consideration public-private cooperation models and the ecosystems around them), with complementary expertise****, from at least 9 Member States*** *or Associated Countries. With the aim of reinforcing technology and industrial capacity as widely as possible across Europe, proposals should include a substantial representation of the most relevant RD&I excellences centres in Europe, with a widespread European coverage and good geographical balance of activities as regards the scope of work. This will ensure the proposals meeting the policy goals of the initiative of supporting the establishment* ***of the future Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre of the European Union.***

"Boosting the effectiveness of the Security Union" - **focus area**

Establishing and operating a pilot for a Cybersecurity Competence network to develop and implement a common Cybersecurity Research and Innovation Roadmap -- **topic**

Call Information

(...) The European Commission has recently adopted a proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres[COM(2018)630]

Considerations on COM(2018)630
European Cybersecurity Industrial, Technology and Research Competence Centre and National Coordination Centres - Contribution to the Leaders' meeting,
September 2018 [5]

*(12) **National Coordination Centres should be selected by Member States**. In addition to the necessary administrative capacity, Centres should either possess or have direct access to cybersecurity technological expertise in cybersecurity, notably in domains such as cryptography, ICT security services, intrusion detection, system security, network security, software and application security, or human and societal aspects of security and privacy. They should also have the capacity to effectively engage and coordinate with the industry, the public sector, including authorities designated pursuant to the Directive (EU) 2016/1148 of the European Parliament and of the Council , and the research community.*

(13) Where financial support is provided to National Coordination Centres in order to support third parties at the national level, this shall be passed on to relevant stakeholders through cascading grant agreements[21].

[21] Note from the editor: Cascading grant agreements -- third parties have a contract with the National Coordination Centre, which is liable towards the EC. No legal and financial validation is required from the EC.

Annex 5 List of Partners

List of Partners			
22	ANSSI	SECRETARIAT GENERAL DE LA DEFENSE ET DE LA SECURITE NATIONALE	France
7	BUT	VYSOKE UCENI TECHNICKE V BRNE	Czech Republic
1	CEA	COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES	France
6	CESNET	CESNET ZAJMOVE SDRUZENI PRAVNICKYCH OSOB	Czech Republic
4	CETIC	CENTRE D'EXCELLENCE EN TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION	Belgium
27	CINI	CONSORZIO INTERUNIVERSITARIO NAZIONALE PER L'INFORMATICA	Italy
28	CNIT	CONSORZIO NAZIONALE INTERUNIVERSITARIO PER LE TELECOMUNICAZIONI	Italy
29	CNR	CONSIGLIO NAZIONALE DELLE RICERCHE	Italy
18	EUT	FUNDACIO EURECAT	Spain
10	Fraunhofer	FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V.	Germany
9	FTS	FORTISS GMBH	Germany
23	IMT	INSTITUT MINES-TELECOM	France
19	IND	INDRA SISTEMAS SA	Spain
43	INOV	INOV INESC INOVACAO - INSTITUTO DE NOVAS TECNOLOGIAS	Portugal
24	INRIA	INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET AUTOMATIQUE	France
30	ISCOM	ISTITUTO SUPERIORE DELLE COMUNICAZIONI E DELLE TECNOLOGIE DELL'INFORMAZIONE	Italy
44	IST	INSTITUTO SUPERIOR TECNICO	Portugal
40	ITTI	ITTI SP ZOO	Poland
2	JR	JOANNEUM RESEARCH FORSCHUNGSGESELLSCHAFT MBH	Austria
16	KEMEA	KENTRO MELETON ASFALEIAS	Greece
32	KTU	KAUNO TECHNOLOGIJOS UNIVERSITETAS	Lithuania
33	L3CE	LIETUVOS KIBERNETINIU NUSIKALTIMU KOMPETENCIJU IR TYRIMU CENTRAS	Lithuania
31	LEO	LEONARDO - SOCIETA PER AZIONI	Italy
36	LIST	LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY	Luxembourg
34	LKA	GENEROLO JONO ZEMAICIO LIETUVOS KARO AKADEMIJA	Lithuania
39	LMT	LATVIJAS MOBILAIS TELEFONS SIA	Latvia
35	MRU	MYKOLO ROMERIO UNIVERSITETAS	Lithuania
41	NASK	NAUKOWA I AKADEMICKA SIEC KOMPUTEROWA - PANSTWOWY INSTYTUT BADAWCZY	Poland
17	NCSR	NATIONAL CENTER FOR SCIENTIFIC RESEARCH "DEMOKRITOS"	Greece
8	NIC	CZ.NIC ZSPO	Czech Republic
42	PPBW	STOWARZYSZENIE POLSKA PLATFORMA BEZPIECZENSTWA WEWNETRZNEGO	Poland
11	SAP	SAP SE	Germany
37	SMILE	security made in LÃ«tzebuerg (SMILE) g.i.e.	Luxembourg
25	TCS	THALES SIX GTS FRANCE SAS	France

List of Partners			
20	TEC	FUNDACION TECNALIA RESEARCH & INNOVATION	Spain
3	TNK	TECHNIKON FORSCHUNGS- UND PLANUNGSGESELLSCHAFT MBH	Austria
12	TUM	TECHNISCHE UNIVERSITAET MUENCHEN	Germany
13	UBO	RHEINISCHE FRIEDRICH-WILHELMSUNIVERSITAT BONN	Germany
14	UKON	UNIVERSITAT KONSTANZ	Germany
5	UNamur	UNIVERSITE DE NAMUR ASBL	Belgium
38	UNILU	UNIVERSITE DU LUXEMBOURG	Luxembourg
15	UTARTU	TARTU ULIKOOL	Estonia
21	VICOM	FUNDACION CENTRO DE TECNOLOGIAS DE INTERACCION VISUAL Y COMUNICACIONES VICOMTECH	Spain
26	YWH	YES WE HACK	France

Annex 6 Cheat Sheets for Technical WPs 4-7

The information in the spreadsheets shown in the following four pages has been extracted manually from the WP descriptions of SPARTA's DoA. Note that partner efforts per tasks are estimates: we evenly distributed the MMs allocated to a partner across all tasks he is involved in. Better estimates may be achievable by factoring in information from quarterly and annual progress reports from the first work period once these are available.

Our main interest, however, was obtain shortlists of the main technical objectives addressed by each tasks and the specific contributions each partner is making. This is a first and tiny step towards an atlas of all capabilities of SPARTA, but even at this rudimentary stage, it simplified our efforts to determine cross-task and synergy potentials. The scheme can be gradually extended by mapping objectives and partner contributions to the cybersecurity taxonomy of the EC's JRC, adding further details about partner capabilities from the descriptions in DoA Part B, and by determining the active contributors from each organization by analysing metadata from the project infrastructure.

All this could feed into a management and decision support system with WP specific dashboards and progress tracking for tasks and general objectives. While some these options will be investigated in future, the actual implementation of such a system is neither the goal nor the objective of T1.4. However, it presents an internal use case that could be subjected for legal and ethical analysis, in particular if interfaced with tools for datamining and Artificial Intelligence.

WP4 Cheat Sheet

WP4 effort /		TSHARK						
	Partner	**MM (plan)**	**T4.1**	**T4.2**	**T4.3**	**T4.4**	**T4.5**	**T4.6**	**role**
	33-L3CE	24	4.00	4.00	4.00	4.00	4.00	4.00	*lead, info analysis, strategic comms*
	31-LEO	23		7.67		7.67		7.67	*decision support, threat intell., sit*
	19-IND	18			6.00	6.00		6.00	*SIEM, threat prevention*
	25-TCS	18		4.50	4.50	4.50		4.50	*security monitoring, virtualization*
	34-LKA	18					18.00		*full spectrum data analytics*
	43-INOV	18		4.50	4.50	4.50		4.50	*intrusion detection, impact assessment*
	41-NASK	16			5.33	5.33		5.33	*info exchange, automat data analysis*
	13-UBO	14			4.67	4.67	4.67		*tech intelligence, information analysis*
	6-CESNET	12			4.00	4.00		4.00	*anonymized data sets*
	39-LMT	12				6.00		6.00	*test, validation*
	44-IST	12		3.00	3.00	3.00		3.00	*data integrity, privacy*
	35-MRU	10					5.00	5.00	*policy, legislation*
	29-CNR	9		4.50		4.50			*collaborative confidential info sharing*
	36-LIST	9		4.50	4.50				*visual analytics, info sharing, collab*
	8-NIC	8				4.00		4.00	*threat intelligence, collab, sharing*
	16-KEMEA	8	1.33	1.33	1.33	1.33	1.33	1.33	*end user, legal, threat intell., sharing*
	18-EUT	8		2.67	2.67	2.67			*defence & decision making provider*
	32-KTU	8		2.00	2.00	2.00		2.00	*info analysis, strategic comms*
	37-SMILE	6		6.00					*testing, validation*
	Effort	251	5.33	44.67	46.50	64.17	33.00	57.33	
	Participants		2	11	12	15	5	13	
	Duration	M01 - M36	M01 - M36	M01 - M36	M01 - M36	M01 - M36	M01 - M36	M01 - M36	
		36	36	36	36	36	36	36	Assumption: effort evenly distributed

	MMs	WP4	T4.1	T4.2	T4.3	T4.4	T4.5	T4.6		**WP4 Cheat Sheet**
WP4	251	**Gen Focus**	**Mgmt**	**Tech**	**H-Tech**	**CollabTech**	**Soc / Politics**	**Inst. Framewk.**	**Indicator**	
WP5	282	**Topic 1**	SpecDemoCase	VisualAnalytics	ThreadIntellig.	Share & Integr..	LegalCompliance.	EndUsers	**Cross-Task (0-4)**	3
WP6	243	**Topic 2**	VerticalDoms	HumanKnowl.	Challenges	Challenge	AssocCouncil	Arbitrage	**Cross-WP(0-4)**	2
WP7	108	**Topic 3**	Validation	PredictModels	Contest	Contest	Workshop	Industry	**Certification (0-4)**	0
Tech. WPs	884						"moot court"		**Platforms (0-4)**	1
		audience /interf	publ / gov adm.	opsec	research	civil soc	industry	ind,acad,policy	**ELSA (0-4)**	2
All WPSs	**1774**	OSS - no							**Verticals**	1
% of SPARTA	14.1	Cert - no (below)					Horizont. / WP2	CSIRTs	**Training**	1
% of TechProgs	28.4	Platf - option					Soc / Pol / Leg	CivSoc / Pol	**Cross-Potential**	3
		ELSA / gov - sugg					LKA (?)	MRU++ (?)	**Comment**	policy, privacy /
Gov. Consideration		**Suggest infrastructure / system of systems assessment by WP5, by inclusion of WP11?**							**Comment**	strategic comms,

WP5 Cheat Sheet

WP5 effort / task		CAPE				
Partner	**MM (plan)**	**T5.1**	**T5.2**	**T5.3**	**T5.4**	**roles**
23-IMT	24	6.00	6.00	6.00	6.00	*lead workpackage/evaluation*
11-SAP	24			24.00		*complex supply chains, agile*
31-LEO	23	7.67		7.67	7.67	*demo cases, validation, (cars, bank egov)*
1-CEA	21	10.50		10.50		*meth, tools f. asss, formal*
14-UKON	21	7.00	7.00	7.00		*vis. analytics for assessment*
4-CETIC	18	6.00	6.00		6.00	*cyber cert ass tools, safety conv*
9-FTS	18	6.00	6.00		6.00	*sec/saf conv modelling*
17-NCSR	18	18.00				*risk tools vert 1 (cars)*
20-TEC	16		5.33	5.33	5.33	*risk analysis f compl sys saf/sec ass*
29-CNR	16	4.00	4.00	4.00	4.00	*risk ass f complex biz srvc*
27-CINI	14	7.00		7.00		*autom sec-anal f multip webserc/mob*
28-CNIT	12	6.00		6.00		*cont'd network monitoring*
13-UBO	10	2.50	2.50	2.50	2.50	*assess training success*
16-KEMEA	10	3.33		3.33	3.33	*assessment iot devices*
18-EUT	10		5.00		5.00	*sec/saf conv vert(cars)*
35-MRU	10	10.00				*tools for end users, tool eval*
38-UNILU	9	2.25	2.25	2.25	2.25	*static / dynamic assess of mobile apps*
41-NASK	8	2.00	2.00	2.00	2.00	*supervision of cert labs*
Effort	282	98.25	46.08	87.58	50.08	
Participants		15	10	13	11	
Duration	M01 - M36	M01 - M30	M01 - M30	M01 - M30	M18 - M36	
	36	30	30	30	19	Assumption: effort evenly distributed between tasks

	MMs	WP5	**T5.1**	**T5.2**	**T5.3**	**T5.4**		**WP5 Cheat Sheet**
WP4	251	**General Focus**	**Tech Proc/Tools**	**Theor / Acad**	**Feas / Econ Via**	**Demo / Valid**	**Indicator**	
WP5	282	**Topic 1**	C_AutomAssess	SafetySsecurity	C_CritInfra	ConversionTools	**Cross-Task (0-4):**	2
WP6	243	**Topic 2**	C_PreAssess	C_Models	OpenSrc, 3rdPty	V_Financial	**Cross-WP(0-4):**	2
WP7	108	**Topic 3**	C_ContdMonit.	C_CommonLang	CrossLayerComplx	V_EGov	**Certification (0-4)**	3
Tech. WPs	884						**Platforms (0-4)**	3
		audience /interf	A_Acad / A_Aert	A_Acad A_Aero A_IndResearch (?)	A_Vert (div)	A_Fin /A_EGov	**ELSA (0-4): 0**	0
All WPSs	**1774**	OSS – no					**Verticals: 3**	2
% of SPARTA	15.9	Cert - Yes					**Training:**	0
% of TechProgs	31.9	Platf - Tools					**Cross-Potential**	3
		ELSA / gov - no						
Gov. Consideration		**Extend WP9 responsibility towards OSS?**					**Comment**	OSS, certification, cmplx analysis
Gov. Consideration		**T5.2 - Docking on the likes of Airbus / Bosch / FHG-SIT?**					**Comment**	WP4, WP10 (clarify)

WP6 Cheat Sheet

WP6 effort / task		HAII-T					
Partner	**MM (plan)**	**T6.1**	**T6.2**	**T6.3**	**T6.4**	**T6.5**	**role**
24-INRIA	42	42.00					*crypto for low end II, integrate in RIOT OS*
27-CINI	25		8.33	8.33	8.33		*sec. orchest. framew, vuln. toler. HW and SW*
7-BUT	24					24.00	*crypto / anonymous / group sig*
2-JR	18			18.00			*form. sec prot verif.*
12-TUM	18		18.00				*defense for SW / virt*
15-UTARTU	18			18.00			*sec prot verif / quantum*
23-IMT	18		9.00			9.00	*sec prot verif*
28-CNIT	12	6.00		6.00			*anls / dev lightweight prots.*
33-L3CE	12					12.00	*practices / standards / end users*
40-ITTI	12				12.00		*infrastructure resilience*
5-UNamur	10					10.00	*GDPR legal analys. f. II / IoT / sensors*
32-KTU	10			10.00			*multi layer sec model, heterog., energy, prototype*
36-LIST	9			4.50		4.50	*orchestr framework, crypto*
38-UNILU	9				9.00		*byzantine prots, last line defense*
9-FTS	6			6.00			*formal evidence lang, formal sec prot verif.*
effort	243	48.00	35.33	70.83	29.33	59.50	
participants		2	3	7	3	5	
duration	M01 - M36	M01 - M36	M01 - M36	M01 - M36	M01 - M36	M01 - M24	
	36	36	30	30	30	24	Assumption: effort evenly distributed between tasks

	MMs
WP4	251
WP5	282
WP6	243
WP7	108
Tech. WPs	884
All WPSs	**1774**
% of SPARTA	13.7
% of TechProgs	27.5
Gov. Consideration	

WP6	**T6.1**	**T6.2**	**T6.3**	**T6.4**	**T6.5**
Gen Focus	**T: SecOS**	**T: LgcyHrdng**	**T: orchestr**	**T: resilience**	**T: PrivByDesign**
Topic 1	CryptoAlg	BinaryAnalysis	Framework	ThreatUncert	AttCert/SecProt
Topic 2	FormalVerif	ProgrTransform	DiffTypesOfTier	CrossSW_Layer	CollectConsent
Topic 3	RIOT-OS	DifficultyMetrics	ID_Mgt/AccsCtl	OSS	DeviceCaps
audience /interf	publ / gov adm.	infosec / cmpl	acad research	acad research	acad research
Cert - no	OSS		OSS	L3CE / WP4 link	priv/leg/hor
OSS T6.1, 6.4			Platf? T6.3?		
Platforms (?)					
Possibly best OSS interface ...No training - academic. Interface with WP9					

	WP6 Cheat Sheet
Indicator	
Cross-Task (0-4)	1
Cross-WP(0-4)	2
Certification (0-4)	1
Platforms (0-4)	1
ELSA (0-4)	0
Verticals	1
Training	0
Cross-Potential	2
Comment	framework, cross SW layer => WP4
Comment	dec. support, . => ELSA

WP7 Cheat Sheet

	WP7 Effort / task		SAFAIR					
	Partner	**Effort plan**	**T7.1**	**T7.2**	**T7.3**	**T7.4**	**T7.5**	**role**
	40-ITTI	24	4.8	4.8	4.8	4.8	4.8	*lead, preliminary description*
	21-VICOM	24	8	8			8	*not specified*
	25-TCS	18			9		9	*decision support, testing*
	20-TEC	14	7				7	*AI threat analysis & modelling*
	12-TUM	12	3	3	3		3	*defence, transparency, methodology*
	5-UNamur	10	5			5		*GDPR legal analysis*
	1-CEA	6		3			3	*performance resilience / benchmarks*
	Effort	108	27.80	18.80	16.80	9.80	34.80	
	Participants		5	4	3	2	6	
	Duration	M01 - M36	M01 - M18	M04 - M30	M04 - M30	M04 - M30	M18 - M36	
		36	18	27	27	27	19	Assumption: effort evenly distributed between tasks

	MMs	**WP7**	**T 7.1**	**T7.2**	**T7.3**	**T7.4**	**T5.5**		**WP7 Cheat Sheet**
WP4	251	**Gen Focus**	**T: ThreatModel**	**T: ReactSecurity**	**T: Explainability**	**T: AI fairness**	**T: Test/Valid**	**Indicator**	
WP5	282	**Topic 1**	RiskAnalysis	DataProtection	HumMachInterf	System. Method	benchmarking	**Cross-Task (0-4)**	2
WP6	243	**Topic 2**		DefenceMech	DecisionSupp	GDPR/H-Rights	3 verticals app	**Cross-WP(0-4)**	1
WP7	108	**Topic 3**		PerfResilience	Transp./Forens	CrossTaskCoop	CrossTaskCoop	**Certification (0-4)**	1
Tech. WPs	884							**Platforms (0-4)**	1
		audience /interf	acad / rsrc	acad / rsrc	acad / rsrc	acad / rsrc	acad / rsrc	**ELSA (0-4)**	0
All WPSs	**1774**								
% of SPARTA	6.1	Cert - no				priv/leg/hor		**Verticals**	0
% of TechProgs	12.2	OSS - no						**Training**	2
		Platfoms - no				UNAMUR		**Cross-Potential**	fairness., transpar., GDPR => ELSA
Gov. Consideration		**Very limited involvement in horizonals-- strengthen WP2 links?**						**Comment**	dec. support, methodology=> WP4