EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR COMMUNICATIONS NETWORKS, CONTENT AND TECHNOLOGY
CNECT.H – Digital Society, Trust and Cybersecurity
H.01 – Cybersecurity Technology and Capacity Building

GENERAL PROJECT REVIEW CONSOLIDATED REPORT

Grant agreement (GA) number:	830892
Project[1] Acronym:	SPARTA
Project title:	Strategic programs for advanced research and technology in Europe
Type of action:	RIA
Start date of the project:	01/02/2019
Duration of the project:	36
Name of primary coordinator contact and organisation:	Florent KIRCHNER (CEA)
Period covered by the report:	from 01/02/2019 to 31/07/2020
Periodic report/Reporting period number:	1
Date of first submission of the periodic report (if applicable):	27/10/2020
Amendments (latest AMD concerning description of the action)[2]	10/07/2020 (AMD-830892-22)
Date of meeting with consortium (if applicable):	01/10/2020
Name of project officer:	Martin UBELHOR
Name(s) of monitors:	– Liisa Past • Cybernetica AS • Kuri Kala OÜ • Government Office, Republic of Estonia – Nils-Gregor LEANDER • RUHR-UNIVERSITAET BOCHUM – EMMANOUIL CHRISTOFIS • self employed • NATO • SHAPE J6 – Pedro INÁCIO • University of Beira Interior

[1] 'Project' means the same thing as 'action'.
[2] Only amendments to the description of the action (DoA; AT21) are relevant for general project reviews since they always have to be carried out against the latest version of the DoA

1. Overall assessment

1. Overall assessment
Project has achieved most of its objectives and milestones for the period with relatively minor deviations.
2. Significant results linked to dissemination, exploitation and impact potential
Project will likely provide results with significant immediate or potential impact in the next reporting period (even if not all objectives mentioned in the Annex 1 to the GA were achieved). The main objectives for the reporting period were achieved and clear progress has been made since the last review. A detailed overall practical demonstration of the applicability and implementation of the whole approach is of paramount importance for the next review. The output in terms of dissemination in scientific venues is in line with expectations. The efforts to produce quality results and synchronize those with other pilots are notable given the context of the pilots and the pandemic. In this review cycle, the consortium gave a good overview of the actions taken in communications and dissemination beyond scientific fora. In the next cycle, it might be advisable to look more at the impact and effects of publicity and outreach and report on both outcomes/impact as well as output/activities. In the future, please be more specific regarding exploitation. Additionally, you might want to consider some sort of consolidation between advisory boards, possibly with other pilots to avoid fatigue among the stakeholders that all pilots are likely to wish to include. WP7 and WP9 include notable work from the review period on attacks on Artificial Intelligence and survey on curricula with respect to cybersecurity. This has led to some of the most notable outputs from the period, including the web-based tools of the work package 9. The collection of the curricula for universities was a good output from this period, as education is one of the very important areas and the online map is a great overview of activities inside the EU (and worldwide). It is an excellent tool to generate impact, although the target audience and possible beneficiaries are unclear. To take advantage of the full potential of such a tool, it would be great to think about more value and information that can be added to such a map (e.g. reviews or ratings, maybe best based on students studying at the places in question). WPs continue as planned and continue to show impact. The progression of WPs with no deliverables in the last six months was made clear in the review meeting and the roadmap shows the necessary flexibility.
3. General comments
The project contributes to the overall picture for EU Strategic Autonomy and Capacity building for the Future EU Cybersecurity Competence Centre and Network of National Competence Centres. The spirits and progress are good, as is the quality of work. Overall, the milestones for the review period were achieved. Most of the Work Packages seem to be progressing well according to the DoA, and deliverables have been mostly submitted on time. For the most recent six months, all of them were delivered on time and are overall of good quality (although some comments are included with this report). SPARTA is reportedly taking the lead of the skills framework section in the context of the work across the 4 pilots and ECSO (see page 88 of the draft of the periodic report) and also taking the lead on the effort to synchronize roadmaps from pilots, which is commendable. Activities, tasks, and processes are moving ahead with the pandemic impacting the work dependant on in-person meetings and travel or access to physical sites. The consortium is encouraged to systematically consider how to move ahead both in terms of working remotely (particularly in designing replacements for the meetings and brainstorming sessions that are not easy to digitize) and in offering pan-European thought leadership on the meaning of cyber security and collaboration during a pandemic. Overall, the consortium has been able to ramp up the SPARTA project with quality and speed. Previous work based on other EU projects has been taken into consideration and build upon this. Additionally, other existing tools have been taken into consideration and built upon, such as MISP. Given the development and DoA of the pilot, these comments focus also on the period ahead to ensure that the project is in a good position as a next patch of deliverables comes up. Also, these remarks are designed to help the project build towards the end goal of the CCN.

The project is encouraged to look beyond the immediate dissemination of information and results and build interactions and networks that can lead toward the CCN. SPARTA's observations can form a basis for providing solid policy recommendations and roadmapping. Linking the conclusions and recommendations as well as the lessons learned to the EU processes, the project can offer valuable insight, practical policy recommendations, and views into stakeholder management.

SPARTA has remarkable flexibility in terms of DoA to push for impact even at these challenging times. Therefore, the project is highly encouraged, perhaps in cooperation with other pilots, to seize the opportunity of the pandemic and the related overnight accelerated digital transition. The pilots are in a unique position to offer post-pandemic vision, advice and ways forward, including on a pan-European policy and strategy level.

It was not clear that the direction of the tools presented during the review session is towards the support for more complex, multi-stage, full-spectrum cybersecurity incidents that traditional cybersecurity functions in organisations are not sufficient and not effective anymore. In other words, the real-world added value of the tools remains to be demonstrated at later stages of the project. While SPARTA has come far in conceptualizing the tools and developing processes, the next step is to see working prototypes or demos in use.

Other pilots seem to also be working a fair bit on certification and standardization; therefore it might be worth cooperating in the area. In addition, it the pilots might be reaching the level of maturity independently where they could further cooperate on tools, the operational use of their platforms etc.

Some of the foreseen risks for the project have materialized in this first year. Risk identification seems to be working, but it is worrisome that some of the materialized risks – such as lack of interest or involvement - are persisting up to month 18. Risk Assessment can be more pragmatic and the implementation of the mitigation measures needs to be clearer. Additionally, externalities such as the current pandemic or global macro trends might need to be included further in risk management.

4. Recommendations concerning the period covered by the report

The consortium and its activities are well set up and in a good position to fulfill their objectives. The review cycle demonstrates clear evidence of progress in the last six months as well as taking on board earlier remarks. The work done and processes undertaken are clearly striving to be coherent, cooperative, practical, and implementable. The Project should pay particular attention to and demonstrate in the future:

1. The concrete ways in which the work contributes to the strategic aims can be highlighted more clearly.
2. Communication between beneficiaries needs additional systematic attention.
3. The unfinished Advisory Board raises concerns.
4. Risk of lack of interest is highlighted and seems to be materializing, the project might need a different approach to engagement.
5. SPARTA has ideas on how to make ELSA mainstreamed and made sustainable; this can be turned into practical work now, in the next 6 months.
6. SPARTA has defined a clear process and are encouraged to be as flexible or granular regarding certification as possible. This lightweight approach is likely to serve best in the fast-moving cybersecurity environment. Furthermore, the project might want to examine the value of certification as such for Europe and cybersecurity.
7. The added value of WP4, WP5, WP6, and WP7: how are they going to be used, by which community? If they are going to be used by the National CSIRTs/CERTs (as it is mentioned in the documents) then the "Operational Impact" has to be identified in WP2. Further elaboration on the operational use of the tools and how that contributes to strategic autonomy would be beneficial.
8. Cybersecurity threat intelligence can provide greater insight into cyber threats, thus should feed all the tools in which the understanding of the threats is crucial for effective assessment and hardening processes. Currently, T-SHARK risks being an information sharing tool (thus an extended usage of MISP-Malware Information Sharing Platform) but has the potential to be a real cyber threat analysis tool that can provide actionable intelligence to National CSIRTs/CERTs.
9. The connections between WPs (if any) was not clearly addressed to demonstrate the continuity and coherency of the Project. T-SHARK (WP4) should feed SAFAIR (WP7) in regard to cyber threat analysis. If specific AI-related threats had been identified by the SAFAIR Team, these should have been communicated to T-SHARK for cyber threat analysis inputs instead of developing the cyber threat analysis model from scratch for SAFAIR. It looks like duplication of effort, possibly miscommunication, and lack of interaction among WPs.
10. Additionally, for the SAFAIR, the virtual environment created in a Cyber Range in order to test the tool towards highly sophisticated cyber attacks, could be found in other Projects such as ECHO for example and it should not be developed from scratch.

SPARTA should take an approach that highlights the interaction, the coherency among various pilots and could

demonstrate the ability to comprehend the overall big picture of the program, and the strategic direction. Though tagging the deliverables as ACCEPTED, many aspects might still be improved with another revision round and uniformization effort.

5. Recommendations concerning future work, if applicable

For the future, in addition to continued attention to the points raised in the previous section, it is key to focus on the bigger picture again to try to maximize impact and realign with the strategic view. This most likely requires closer collaboration with the other pilots, ENISA and ECSO, and national agencies as well as the European Commission. Many of the observations, if bolstered and generalized, are valuable to help build the future approach to CCN.

The roadmap is well-positioned and realistic within the schedule. Given the changes and surprises of 2020, it is worth approaching it as a living document with less concern for published versions. This would be one of the ways to harness the opportunities of COVID-19. SPARTA is taking the lead on synchronization, which is key during the pandemic and in accounting for the new normal.

Looking ahead, more attention is suggested on the following:
1. Further development and consideration of risk management. This means both accounting and mitigating more for externalities as well as more elaboration on all risk management measures in the next review cycle. Some of the reviewers feel the risk tables were hurried through and would benefit from more focus. Some recommendations on particular risks are outlined above already. Going ahead, it would be advised the partners help more actively mitigate the risk that materialized for WP2 regarding the "involvement of WP3 - WP6 in the WP focusing on Ethical, Legal and Societal aspects";
2. The adverse effects of the pandemic are clear and the impact on the original DoA has been minimized. The reviewers would challenge the consortium to also grasp the inherent opportunities (as described previously) and treat COVID-19 as an extreme test scenario for the creation of a network of experts, eventually trying to go the extra mile to keep on track (instead of postponing, which seems to be a safer approach for many projects) and describe the lessons learned in the meanwhile. The use of online tools is probably a good lesson to be learned from the previous few months that should be applied in the future;
3. Keep up with the work of making the results of work packages (WP) more usable, e.g., via the development of simple to use tools such as the ones from WP9;
4. Identification of any operational use of the work done and validation with the appropriate national authorities on the need for practical outputs. As you are moving ahead, the impact on the operational community (eg. national CSIRTs/ CERTs as well as industry) should be addressed.
5. Clearer interaction among WPs, including further use of the outcome of the WPs in support of the other WPs.
6. Information exchange requirements need to be identified for each tool at different levels.
7. Specific acceptance criteria should be identified for each tool. As an example, for the T-SHARK it is mentioned that it will be able to provide a prediction of cyber and information threats by mapping future threats. What exactly is the “actionable” intelligence that T-SHARK can provide and how is this linked to National CERTs/CSIRTs activities (how does it support effective cyber defence)? Also, how does SAFAIR bolster defensive and reactive mechanisms designed to ensure resilience against the new, complex cyber-threats identified in D7.1? For more, please see also comment in previous section that cyber threat analysis should have come from T-SHARK.
8. It would be advisable for the next review to focus on the demonstration of the application of the tools to specific use cases, even if in a prototype or demo stage. A practical demonstration is essential, particularly as use cases (and sub cases) are documented. Hopefully, the toolset has reached that maturity by the next review cycle. In the case of SAFAIR, for example, the mechanisms and tools will need to include testing of the functionality of AI, the decisions made by AI, and the ability to trace back those decisions to the inputs, paving the way to a better understanding of AI. Otherwise, we will only review the theoretical aspect of each tool and the theoretical application which is absolutely great. However, the practical implementation and usage is the final aim and the real impact.

2. Objectives and workplan

1. Is the progress reported in line with objectives and work plan as specified in the DoA? If there are significant deviations, please comment.	Yes
In terms of milestones and objectives, the progress is, despite COVID, in line with the objectives and the work plan with minor deviations. The work performed thus far contributes to the progress of the project as specified in the DoA. There are understandable technical/logistical deviations when it comes to events and travel due to COVID. The consortium is encouraged to take advantage of the accelerated digital transformation we are encouraging both in terms of online events and analysing the impact on the ecosystem. At the time of writing of this report, the reviewers were nonetheless confused because the status of task 2.2 is not completely clear.	
2. Are the objectives of the project still scientifically and /or technologically relevant?	Yes
The objectives are even more scientifically and technologically relevant now. The objectives of the project provide scientific and technological breakthrough potential and they are still achievable within the time and resources available to the project. The motivation for the call where this project was accepted in is still very relevant. The need to specify and build a cyber security competence centre is relevant, as well as the need to effectively train people in cybersecurity, both covered in the project. Moreover, the programs identified in the scope of the project are as relevant nowadays as they were at the time of the call and they will most certainly remain relevant during the lifespan of the project.	
3. Are the critical implementation risks and mitigation actions described in the DoA still relevant?	Yes
The consortium is well aware of the risks and is encouraged to continue to creatively mitigate them, including the unforeseen COVID pandemic. While the project has managed that risk with minimal effect on the original DoA, there are ways to use the virus to the advantage of the objectives. The critical implementation risks and mitigation actions described in the DoA have not disappeared and as suggested in the previous remarks, dynamic and comprehensive risk management is called for. Some of the foreseen risks for the project have materialized in the first 18 months of the project and some actions were spawned in reaction to their identification, which shows their relevance. Please see the overall assessment for more details.	
4. Have the pilots/case studies started to showcase innovative results as described in the DoA?	Partially
The pilots/case studies have started to showcase innovative results as described in the DoA. However, they are in too early a phase to clearly demonstrate the innovative results. Results, prototypes, and deeper demos are expected in the next reporting period. The pilots and technical WPs have made substantial progress. The T-SHARK project is going well but has yet to show how much it can really be of practical use. SAFIAR is an impressive project that tackles the fundamental questions of AI in general and with respect to security in particular. The reviewers would like to see more comparison with approaches outside SPARTA and, as this is a highly competitive project, this is an excellent area for not only doing research within SPARTA, but build networks. The consortium is, therefore, encouraged to keep a close eye on the market and scientific results worldwide. For example, in regard to T-SHARK, automation and predictive security is a crowded race. Similarly, elections are a tricky test case because of so many differences and variables as well as the scheduling of elections. Additionally, the information space can be a fair bit different from the cybersecurity domain. Therefore, it would be great to hear more about the actual meaning and content of the work in the next review cycle. How is T-SHARK unique or builds (rather than competes with) private and national initiatives? For example, there is a fair bit of election work in the US (DHS's CISA, CIS's EI-ISAC) to learn from. The objective of this pilot is to gather input for the cybersecurity competence center (CCN). Analysis on how to start a CCN, its instruments and governance structure, as well as some lessons learned from this process has commenced.	
5. Have the ethics deliverables due for the current period been adequately addressed and approved?	Yes
The ethics deliverables due for the current period have been adequately addressed and approved. Ethics related deliverables have been submitted on time and approved with some lack of clarity around task 2.2. The consortium might be able to mainstream the ELSA deliverables beyond their activities when cross-fertilizing ideas with work on young researchers and Ph.D. students.	

The management structure specifies an Ethics Committee and an Ethics Officer. Several work packages handle aspects related to ethics, namely WP2 and WP14.	
6. Have the comments and recommendations from previous project reviews been taken into account?	Yes
The consortium shows an active interest in comments and has been looking to make improvements. The comments and recommendations from previous project reviews have been taken into account reasonably well. D6.1 was tagged as ACCEPTED, but the consortium revised it anyway. We were only able to spot a noticeable difference in the Conclusions, in which a small subsection of "Final remarks and recommendation" was added. It is hoped the consortium will be able to still address the respective comments better in the future. The reviewers are comfortable with accepting D13.1 and D13.2 after the modifications. D11.1 has seen substantial modifications to cope with comments (which is commendable) but would still benefit from another round of revisions or proofreading to improve writing quality, assuming that this is a public deliverable. Language is colloquial at times, and text justification is not coherent with the other deliverables of this project. There are several typos or errors in the text (e.g., opening or closing brackets without their counterpart). Take, for example, sentences in the Conclusion: "It is now time that the European Union take a closer look at all these schemes and initiatives and try to push a European SME’s certification." (writing quality); "It can be the beginning of a great cybersecurity journey for a company" (colloquial).	

3. Impact

1. Does the work carried out contribute to the expected impacts detailed in the DoA?	Yes
In the future, please show further how this work helps to move toward CCN. More understanding of the functions of the developments and a clear demonstration of the impact are required. The work carried out lays out many of the foundations for the expected impacts in the DoA, namely in terms of State-of-the-Art, identification of technologies (e.g., identification of technologies for securing information systems), devising models and structures (e.g., management structure for a Cyber Security Competence Center/Network) foreseen for the project and some of the Work Packages have started to produce outputs aligned with those expected impacts.	
2. Does the work carried out follow the plan detailed in the DoA to enhance innovation capacity, create new markets opportunities, strengthen competitiveness and growth of companies, address issues related to climate change or the environment, address industrial and/or societal needs at regional level or bring other important benefits for society? Give information on the relevant innovation activities carried out (prototypes, testing activities, standards, clinical trials) and/or new product, service, reference materials, process or method (to be) launched to the market, if any.	Yes
The work carried out is in line with the DoA and, up to now, contributes to these aspects in a broad manner. For example, it is discussed how improving cybersecurity will contribute to a safer society and more trust, also in line with the project call, but this is yet to better materialize. The work carried out follows the plan detailed in the DoA to enhance innovation capacity, create new market opportunities, strengthen competitiveness and growth of companies. However, a more detailed demonstration of the innovation needs to be presented in the next review. Prototypes' testing activities and acceptance criteria have not been developed yet, so the reviewers are looking forward to seeing concrete examples soon. Work on cybersecurity curricula might help close the need for specialists working in the cybersecurity industry, which will indirectly contribute to the competitiveness of companies. On the other hand, certification will also have an impact on the competitiveness of and trust in companies, answering as well to a notable societal need.	
3. Does the work carried out contribute towards European policy objectives and strategies and have an impact on policy making?	Yes
The work carried out contributes towards European policy objectives and strategies and can have an impact on policy making. In the next review, further synthesis on the practical and measurable effect on Europe is expected The call in which the project was accepted specifically tackles European policy objectives and strategies, with potential impact on policy making. The objectives to lay out the grounds for a cybersecurity centre or define roadmaps for actuation in terms of cybersecurity alone would justify the positive answer to this question.	
4. Does (or will) the work carried out have an impact on SMEs?	Yes
From a broad perspective, any project contributing to the overall European cybersecurity will benefit SMEs, as they are increasingly supported by or operating in the digital realm. Companies working on the emerging Internet of Things and technological solutions will greatly benefit from certification, which is part of the focus of the project. Impact on SMEs should be better demonstrated in the future review cycles, including in terms of getting the practical tools to that target audience.	
5. Have the beneficiaries reached gender balance at all levels of personnel assigned to the action? If not, have the reasons been explained in the periodic report?	Yes
Most deliverables have editors or contributors of both genders and some of the partners (and project) are actively motivating initiatives aiming to attract women to the area (e.g., Women in SPARTA initiative). Consider providing a better description on mainstreaming activities regarding gender balance in the next review period.	

4. Implementation

1. Has the project been efficiently and effectively managed?	Yes
No evidence to the contrary was found in the documentation, particularly in the draft of the periodic review. All in all, the project has been managed well, particularly given the externalities of 2020. The consortium is aiming, to a large extent, to maximize impact and be inclusive through networking. The fact that ANSSI is not contributing at all might be critical as it fits the picture that SPARTA so far has not found a way to integrate government agencies across Europe. This is certainly not an easy task and can become a real problem in the future. The same holds for the external advisory board.	
2. Is the management of the project in line with the obligations of beneficiaries (including ethics and security requirements, risk and innovation management if applicable)?	Yes
As far as can be assessed, the management of the project is in line with the obligations of beneficiaries. Addressing the risks which have materialized and persist will be crucial going forward. The management structure is adequate for the objectives and for a consortium of the size of this project. Ethics, risk, and innovation all covered by the management structure and by the project work packages per se.	
3. Is the contribution of each beneficiary in line with the work committed in the DoA? (applicable only to multibeneficiary projects)	Partially
As far as can be assessed, most of the beneficiaries seem to be contributing actively to the project in accordance with the DoA. Justifications provided for under-performing partners, provided in the draft of the periodic report, are mostly acceptable. The exceptions are: 1. ANSII, which does not seem to have contributed so far; 2. NASK, which mentions that insufficient understanding of NASK goals in these work packages by allocated personnel was identified as the core reason for under-performing (see page 134 of the draft of the periodic report).	
4. Have the beneficiaries disseminated project results (foreground) in scientific publications as planned in the DoA (including the deposition of publications in open access repositories)? Do they include a reference to EU funding?	Yes
Beneficiaries reported 57 accepted papers in the review meeting. While there is always room for improvement, they have been publishing papers in high quality venues and actively participating in scientific fora to disseminate findings of the project. Publications randomly surveyed all included reference to EU funding and are readily available for download from the project website (see https://www.sparta.eu/papers/). Please see under general remarks regarding dissemination to a wider audience. Also, it would be most useful to hear during the next review which of the publications are uniquely SPARTA and would not have happened if there was no project.	
5. Have the beneficiaries disseminated and communicated project activities and results by other means than scientific publications (social media, press-release, the project web site, video/film, etc) as planned in the DoA? Do they include a reference to EU funding?	Yes
The beneficiaries disseminated and communicated project activities and results by other means than scientific publications (social media, press release, the project website, video/film, etc) as planned in the DoA. The project has set up a website, a Twitter account, a LinkedIn group and an Instagram account to communicate the project (see D12.3). The project is actively producing content and references on social media. The website is at https://www.sparta.eu/. It contains no links to (or integration of) social accounts, but it was improved since the last review (useful sections and tools were added to the website). However, there is no information SPARTA friends and associative projects on the website at the time of assessment. The Twitter handler is @sparta_eu. It is a very active Twitter account, which already gathered a substantial number of followers at the time of this review (average of more than one follower per day, totalling 1020 followers). Commendably, some content is retweets of similar projects, in line with the call's requirements. The LinkedIn website is https://www.linkedin.com/company/sparta-eu and it has 397 followers at the time of this review. The Instagram account is at https://www.instagram.com/sparta_eu/, with 70 publications and 176 followers. CyberCompetenceNetwork brand has been created with a website where SPARTA is listed and is actively contributing	

to. Press releases and podcasts were also prepared in this reporting period, some of them mentioning COVID-19. The project also produced several videos that are available on the website. However, as in the previous review, the consortium is greatly encouraged to seek thought leadership and publication of results outside their own channels, be it other (popular scientific or cyber security) media channels or any number of diverse avenues.	
6. Has the plan for the exploitation and dissemination of the results (if required) been updated and implemented as described in the DoA, in particular as regards intellectual property rights? Is it appropriate?	Yes
The plan for the exploitation and dissemination of the results has been updated and implemented as described in the DoA, in particular as regards intellectual property rights. Plans for exploitation (D10.4) and dissemination (D12.3) were delivered at month 12 and were accepted in the previous review period. An update for these plans is expected for January 2021. The consortium is requested to establish a clearer standard and objective with respect to publications. While there is no easy and consistent way to evaluate the quality of publication venues or the impact of publication, SPARTA should at least be having this discussion (e.g. CORE ranking could be used (ITTI did give CORE rankings) and citation numbers could be considered). Potentially the publication data on the website could be better sorted to make it better accessible.	
7. Has the data management plan (DMP) (if required) been updated and implemented? Is it appropriate?	Yes
The data management plan (DMP) has been updated and implemented. The data management is deliverable 10.2 and is currently defined (by the consortium) as a living document, which is appropriate given the context of the project.	
8. Have the proposed institutional changes been appropriately promoted?	Not applicable
Overall, the project is managed well and there is no specific institutional change.	

5. Resources

1. Were the resources used as described in the DoA and were they necessary to achieve its objectives? If there are deviations from planned budget, have they been satisfactorily explained? Have they been used in a manner consistent with the principle of sound financial management (in particular economy, efficiency and effectiveness)?	Yes
The resources were used as described in the DoA and were necessary to achieve its objectives as far as can be assessed. There are small deviations, which are satisfactorily explained. An analysis of a draft of the periodic report showed that expenditures seem to be in line with expectations for most of the beneficiaries. Deviations in terms of man-month have been mostly justified with shifting between junior and senior personal, leading to the same final expenditures in terms of human resources.	

Annex 1

Expert opinion on deliverables

Deliverable number	Deliverable name	Status	Comments
D1.1	Bootstrapping a CCN pilot	Accepted	This deliverable was assessed and tagged as ACCEPTED in the previous review period. Well documented. Meeting the objectives.
D1.2	Lessons learned from internally assessing a CCN pilot	Accepted	This deliverable was assessed and tagged as ACCEPTED in the previous review period.
D2.1	Ethical, legal, and societal aspects	Accepted	Well documented. Meeting the objectives. This deliverable was assessed and tagged as ACCEPTED in the previous review period.
D2.2	First internal ELSA audit and supervision report	Accepted	This deliverable was assessed and tagged as ACCEPTED in the previous review period. Well documented. Meeting the objectives.
D3.1	Initial SPARTA SRIA (roadmap v0.1)	Accepted	This deliverable was assessed and tagged as ACCEPTED in the previous review period. A clear demonstration of the overall capability should be planned for the next review.
D3.2	Updated SPARTA SRIA (roadmap v1)	Accepted	This deliverable was assessed and tagged as ACCEPTED in the previous review period. A clear demonstration of the overall capability should be planned for the next review
D4.1	Cybersecurity threat intelligence common data model	Accepted	A clear demonstration of the overall capability should be planned for the next review. Threat Analysis from ECHO should be taken into consideration On specifics and for the future iterations: - "The EBIOS risk management rocess" > "The EBIOS risk management process"; Figure 4.1 does not really contribute to the discussion and could be safely removed from the document. - The quality of figure 4.2 is not adequate. - Using the designation "similar-sha256" might not convey the best meaning, given the way one reads the attribute...
D5.1	Assessment specifications and roadmap	Accepted	This deliverable was assessed and tagged as ACCEPTED in the previous review period.
D6.1	Security-by-design framework for the intelligent infrastructure	Accepted	This deliverable was assessed and tagged as ACCEPTED in the previous review period. A clear demonstration of the overall capability should be planned for future reviews.
D7.1	AI systems threat analysis mechanisms and tools	Accepted	A clear demonstration of the overall capability should be planned for future reviews.
D7.2	Preliminary description of AI systems security mechanisms and tools	Accepted	This deliverable was assessed and tagged as ACCEPTED in the previous review period. A clear demonstration of the overall capability should be planned for future reviews.

Deliverable number	Deliverable name	Status	Comments
			For future iterations, please note: - The inclusion of mathematical expressions as images (see page 41) is not adequate for such a technical document. I would say that the same applies to algorithms. - The quality of many images of this deliverable is not adequate. - Though the quality of writing of this deliverable is good, it would benefit from proof-reading, mostly section 4.2.2.1. Minor details such as the use of apostrophe or inconsistency of title heading capitalization deserve attention too.
D8.1	Initial results of the clustering, platforms, and ecosystems activities	Accepted	This deliverable was assessed and tagged as ACCEPTED in the previous review period.
D9.1	Cybersecurity skills framework	Accepted	This deliverable was assessed and tagged as ACCEPTED in the previous review period.
D9.2	Curricula descriptions	Accepted	Thought the quality of writing is good on average, it fluctuates sometimes, e.g., "For a sake of time and resources, the cover of all the existing curricula was not feasible.", "Over 61 curricula, only 5 are multi-university ones." Other typos and corrections needed: * "Pedro Adao" > "Pedro Adão"; * "Table of Content" > "Table of Contents"; * The quality of figure 3.1 is not adequate; * "to be add to ”Information" > "to be added to the ”Information"; * Figures such as Figure 6.13 are not really the best means to clarify the discussion and can be safely avoided in these documents.
D10.1	Pre-existing components identification documentation	Accepted	This deliverable was assessed and tagged as ACCEPTED in the previous review period.
D10.2	Data management plan (DMP)	Accepted	This deliverable was assessed and tagged as ACCEPTED in the previous review period.
D10.3	Project results description documentation	Accepted	This deliverable was assessed and tagged as ACCEPTED in the previous review period. It would be useful to hear back about how well these work for the participants.
D10.4	Sustainability and exploitation plan	Accepted	This deliverable was assessed and tagged as ACCEPTED in the previous review period.
D11.1	International and national cybersecurity certification initiatives	Accepted	This deliverable was tagged with a REQUEST_FOR_REVISION in the previous revision round. A revised version of the deliverable was made available in June. It addresses comments in a way allowing accepting it at this point, although it would still benefit from another revision round to improve the quality of writing (provided that this is a public deliverable). Language is colloquial at times, and text justification is not coherent with the one used in other deliverables of this project. There

Deliverable number	Deliverable name	Status	Comments
			are several typos or errors in the text (e.g., opening or closing brackets without their counterpart). E.g., of sentences in the Conclusion chapter: "It is now time that the European Union take a closer look at all these schemes and initiatives and try to push a European SME's certification." (quality of writing); "It can be the beginning of a great cybersecurity journey for a company" (colloquial). In terms of content, the Inclusion of advice on the value of cybersecurity certification would benefit all.
D11.2	Cybersecurity compliant development processes	Accepted	This deliverable discusses a proposal for a process-oriented certification in a competent manner. Though I consider the deliverable to be generally well written, it would still benefit from some proof-reading. Lists, especially, should at least be handled coherently within the document.
D12.1	Dissemination and communication plan, updates, and evaluation	Accepted	This deliverable was assessed and tagged as ACCEPTED in the previous review period and is to be constantly updated.
D12.2	Internal and external IT communication infrastructure and project website	Accepted	This deliverable was assessed and tagged as ACCEPTED in the previous review period.
D12.3	Updated dissemination and communication plan and evaluation – v1	Accepted	This deliverable was assessed and tagged as ACCEPTED in the previous review period and is to be under constant revision. Well done!
D13.1	Project quality plan	Accepted	This deliverable was tagged with a REQUEST_FOR_REVISION in the previous revision round. A revised version of the deliverable was made available in June. It addresses comments sufficiently at this point.
D13.2	Innovation management plan	Accepted	This deliverable was tagged with a REQUEST_FOR_REVISION in the previous revision round. A revised version of the deliverable was made available in June. It addresses comments sufficiently.
D13.3	Risk assessment plan	Accepted	This deliverable was assessed and tagged as ACCEPTED in the previous review period and is more relevant than ever - might be worth including externalities to a greater degree. More insight on the "High" Risks should be taken into consideration and be presented to reviewers in order to demonstrate a clear understanding of the High Risks from the Consortium to avoid surprises
D14.1	DU - Requirement No. 1	Accepted	This deliverable was assessed and tagged as ACCEPTED in the previous review period.
D14.2	H - Requirement No. 2	Accepted	This deliverable was assessed and tagged as ACCEPTED in the previous review period.
D14.3	POPD - Requirement No. 3	Accepted	This deliverable was assessed and tagged as ACCEPTED in the previous review period.

Annex 2

Expert opinion on milestones

Milestone number	Milestone name	Achieved	Comments
MS1	Successful SPARTA project start	Yes	This milestone was assessed in the previous review round and tagged as being successfully achieved.
MS2	Successful SPARTA CCN launch	Yes	The CCN started well and is gaining increasing impact and visibility. However, more can be done in the future to offer lessons learned for the European CCN.
MS3	Successful community and exploitation initial mappings and engagement	Yes	Based on the deliverables mentioned as means of verification and their contents, this milestone is achieved. Sparta is doing well in directing effort to building up its network as well as getting collaborations with the other pilots started.