1. **SPARTA SELF-ASSESSMENT AND SUGGESTIONS**
2. **Explanation/instructions**

This document aims at collecting information from the 4 Pilots, ECSO and ENISA (here referred as contributors) on their self-assessment of ongoing, already performed activities and identify possible ways forward in key cybersecurity areas of EU action. The document presents nine main strategic axis and associated topics proposed by the contributors. Each axis is described in an explanatory table with information on policy background, scope, objectives, targets, among other details. An additional table is provided for each axis with further information on the associated topics collected during the first step of the exercise. The contributors are now requested to validate this information for each axis and continue with the self-assessment on what was already delivered, ongoing or planned, possible ways forward and the potential actors proposed for future actions.

The following table provides an explanation of what is expected from contributors on the topics presented for each strategic axis.

|  |  |
| --- | --- |
| **COLUMNS** | **DESCRIPTION** |
| **TOPIC** | Name of the topic. |
| **DESCRIPTION** | A brief description of the topic. |
| **SELF-ASSESSMENT – COMPLETED** | The column includes information about the actions/deliverables already finalised for each topic. In case the cell is pre-populated with information, please consider validating it. Please reference the deliverable code of activity name to exemplify. In the case the topic is reviewed in a specific chapter of a document, please reference the number. Please keep the information brief. |
| **SELF-ASSESSMENT – ON GOING** | This column includes information about the actions/deliverables that are ongoing and not finalised for each topic. In case the cell is pre-populated with information, please consider validating it. Please reference the deliverable code of the activity name to provide examples. In the case the topic is reviewed in a specific chapter of a document, please reference the number. Please keep the information brief. |
| **POSSIBLE WAYS FORWARD** | Use this column to provide information and make recommendations on possible ways forward for each of the topics. This information should consider actions and deliverables for future initiatives to be performed by the Competence Community, Centre and Network. |
| **ACTORS** | Please suggest any actors involved in the activities/actions recommended for possible ways forward identified in the previous column. |

Contributors are also asked to validate the information for the Axes table included in the yellow boxes. Furthermore, contributors may also propose other topics within each of the nine axes.

The axis proposed are the following:

1. Resilience of EU critical infrastructure;
2. Resilience of the digital supply chain;
3. Stimulation of the EU cybersecurity market;
4. Improving EU technological sovereignty in cybersecurity;
5. Human and social perspective;
6. Cybersecurity awareness;
7. Capacity building (demand and supply);
8. Strategic priorities for cybersecurity research, innovation and uptake;
9. European cybersecurity cooperation structures, approaches and actors;
10. **SPARTA self-assessment and input**

|  |  |
| --- | --- |
| **AXIS** | **RESILIENCE OF EU CRITICAL INFRASTRUCTURE** |
| **POLICY**  **CONTEXT/**  **AREAS OF**  **EU ACTION** | Resilient infrastructure and critical services: The EU’s critical infrastructure and essential services are increasingly interdependent and digitised. All Internet-connected things in the EU, whether automated cars, industrial control systems or home appliances, and the whole supply chains which make them available, need to be secure-by-design, resilient to cyber incidents, and quickly patched when vulnerabilities are discovered. |
| **SCOPE** | This axis addresses one of the main areas of EU action identified in the EU's Cybersecurity Strategy for the Digital Decade as "resilient infrastructure and critical services". It highlights the importance of improving the resilience of EU critical infrastructure supporting the delivery of essential services in the event of a cybersecurity incident. It refers to the NIS Directive and to securing the next generation of mobile broadband networks (5G security). The topics associated with this axis should cover security aspects that improve the resilience of the EU critical infrastructure in sectors identified in NIS directive. Topics include the research and development of new approaches, systems, tools, processes aiming at the assessment, management and mitigation of risks and improvement of all participants' maturity in securing its digital infrastructure. |
| **OBJECTIVES** | * EU Critical Infrastructure resilient and prepared to deal with cybersecurity threats. |
| **WHO** | Focus group on:   * Supply-chain security. * Specific vertical elements. (e.g. finance, healthcare and food distribution) * Cyber threat intelligence. |
| **TARGETS**  (e.g. through coordination, legislation, funding) | * Establishing a joint taskforce (see 6) on digital supply-chain resilience and security * Designing and publishing European doctrine elements * Investing significant HE and DEP funding on multi-disciplinary projects on the topic. Managing a coherent, competitive portfolio on this topic, ranging over geopolitics, informatics, electronics, sociology, ergonomics, etc. |

**Comments from SPARTA on the Axis:**

No focus group exists on this topic. SPARTA’s Certification Activities, T-SHARK, SAFAIR and CAPE Program perform relevant work on this toping under the current DoA. Contributions from an extended DoA might cover results maturation and field validation, prospective work on innovative use of tooling in supply-chain design and operation (cyber-centaur), and exploratory work on new approaches to certification.

**TOPICS TABLE FOR THE AXIS: RESILIENCE OF EU CRITICAL INFRASTRUCTURE**

| **TOPIC** | **DESCRIPTION** | **SELF-ASSESSMENT –**  **COMPLETED** | **SELF-ASSESSMENT -**  **ON GOING** | **POSSIBLE WAYS FORWARD** | **ACTORS** |
| --- | --- | --- | --- | --- | --- |
| **RISK ASSESSMENT AND MITIGATION METHODS FOR SUPPLY CHAINS** | This topic explores the adoption of risk management practices in the protection of critical infrastructure. For example, the introduction of processes, activities and tools related to the continuous assessment of cyber risks and threats and consequent mitigation measures. |  | The CAPE program proposes tools to validate software, including aspects relevant for the software supply chain (e.g. vulnerabilities in libraries and build processes). It covers the entire software lifecycle. It includes certification (in the CC sense). Several tools propose impact and risk assessment, and potential mitigation measures. (D5.\* deliverables). Many of the tools are available as open source.  T-SHARK Program will establish a Cybersecurity Threat prediction framework (D4.4) and legal framework (D4.5). | The tools are only partially integrated at this stage. Better integration and additional coverage analysis would provide better assessment and mitigation. Gaps are still apparent in some parts of the software life-cycle (e.g. end of life) and for certain technologies (e.g. interpreted languages such as python – probably difficult to cover) and new languages such as rust (probably a very good target).  In CAPE several risk management approaches, including optimal countermeasures selections could be developed tailoring those to specific EU critical infrastructures | Major software developers, cloud operators. |
| **THREAT LANDSCAPE AND ANALYSIS** | This topic considers the design, development and/or implementation to collect, analyse and share threat information. Includes processes for advance warning and detection of threats, threat tools, techniques and procedures (TTP) as well as the profiling of malicious behaviour, actors and trends. | T-SHARK Program establish a Cybersecurity Threat Intelligence Framework. D4.1: Cybersecurity threat intelligence common data model  SAFAIR provided a threat analysis for AI systems (D7.1) | T-SHARK will provide a cybersecurity threat prediction framework (D4.4) regrouping approaches methods and processes to provide comprehensive prediction of threats. |  |  |
| **INCIDENT DETECTION, ANALYSIS AND REPORTING** | This topic refers to adopting processes and protocols for the sharing of threat data and information among participants of a supply-chain or operators of essential services. It also includes the promotion of incident reporting to improve preparedness and resilience of networks and information systems, and the sharing of incident information with industry cooperation groups such as ISACS and CSIRTs. | T-SHARK Program established a Cybersecurity Threat Analysis model (D4.2) | T-SHARK prediction framework will be coupled with a threat intelligence methodology (D4.3, CO) as well as a cybersecurity threat prediction legal framework and a visual analytics system for cybersecurity threat analysis (D4.6). |  |  |
| **STANDARDISATION AND CERTIFICATION** | This topic considers the research and preparation of standards and certifications for ICT products and services. Includes initiatives aiming at increasing the trust from consumers in the adoption of ICT products and services through certification. Moreover, the research of new standards to achieve interoperability of new technologies bringing significant benefits to both industry and consumers. | D11.1: International and national cybersecurity certification initiatives.  D11.2: Cybersecurity compliant development processes. | Discussion are continuing on product oriented certification versus process oriented certification (see D11.2). Also the topic of incremental product certification and continuity of certification is a key discussion topic (see D11.1). Idea of a network of evaluation facilities in support of incremental certification will be reported in D11.3.  The CAPE program is providing tools and demonstration of the integration of certification techniques in software development. | Need to extend the discussion to the other pilot project with the creation of a cross pilot working group on certification. | Other pilots |
| **MATURITY ASSESSMENT** | This topic acknowledges the importance of conducting regular maturity assessment of entities maintaining EU critical infrastructure in the level of resilience to cybersecurity incidents and threats. This topic includes the adoption of various techniques such as penetration testing, security testing and threat modelling. |  | Some of the CAPE tools focus on continuous assessment and are thus of interest to maintain a strong cybersecurity level all along the lifetime of critical software, particularly in a context where tools have a long life expectancy and where remediation opportunities (e.g. patching or deployment of a new configuration) might be scarce. | Develop a link between maturity assessment and continuity of certification. |  |
| **ADVERSARIAL SECURITY** | This topic explores novel solutions in adversarial security in various contexts such as SCADA/ICS systems, machine-learning systems used by OES. | SAFAIR aims at providing mechanisms and tools for AI-based systems used in any infrastructure. A preliminary description can be found in D7.2 and a first demonstration was provided in D7.4. | One of the CAPE tools deals with adversarial machine learning for detection.  A final version of SAFAIR AI systems security mechanisms and tools will be delivered in D7.5 |  |  |
| **MULTIDISCIPLINARY** | A topic dedicated to the investment in projects covering multi-disciplinary aspects of cybersecurity. Managing a coherent, cooperative portfolio on this topic, ranging over geopolitics, informatics, electronics, sociology and ergonomics. | WP 2 (and partly also the programmes) try to address issues from a multi-stakeholder and multidisciplinary perspective. The multi-stakeholder perspective tries to take into account the different interests and influences of decision-makers, users and affected parties. This includes social science, law and ethics perspectives to complement the informatics perspective. |  |  |  |
| **DATA HANDLING REQUIREMENTS** | A topic dedicated to the analysis and specifications/ clarifications about data requirements like: which information needs to be made available, retention periods, impact of handling confidential information, access requirements. | WP4 Task 4.4. developed approaches for data sharing based on data usage control approaches, the same advocated for GAIA-X infrastructure  D4.1 Cybersecurity threat intelligence common data model | T-SHARK will provide a collection of methods and procedure for how TI should be organized and executed in end user organisation (D4.3). | Promote application of data usage control approaches in several fields, having data (and data centric policies) as first class citizen. |  |
| **HARMONISE MANDATORY INCIDENT REPORTING** | This topic refers to the research and development of innovative and efficient ways to coordinate and unify the different applicable regulations and to harmonize mandatory incident reporting procedures to reduce time and costs. |  | D4.5 Cybersecurity threat prediction legal framework, will report on the outcome of T-SHARK analysis and suggest recommendations for further cybersecurity and regulation development. |  |  |
| **CROSS-SECTORAL RISK ANALYSIS AND THREAT INFORMATION EXCHANGE** | A topic exploring innovative and efficient ways to exchange cross-sectoral risk analysis and threat information in Europe. |  | D4.3 Comprehensive full-spectrum cybersecurity threat intelligence methodology by providing tools, methods, skills and procedures for how TI should be organized and executed. | This topic should be further extended. SPARTA cooperates with EU Ubinet and E-CORRIDOR projects that foster ISACs that are cross sectorial, avoiding silos. |  |
| **OTHER TOPICS** |  |  |  |  |  |
| **Cyber insurance** | A topic on the interplay between risk and economy and society, involving several actors. It is also relevant to study how market regulated cyber insurance frameworks could improve the common security measures. |  |  | In CAPE several risk models and cyber insurance models are currently under development. |  |

|  |  |
| --- | --- |
| **AXIS** | **RESILIENCE OF THE DIGITAL SUPPLY CHAIN** |
| **POLICY**  **CONTEXT/**  **AREAS OF**  **EU ACTION** | A reinforced presence on the technology supply chain: With its planned financial support for cyber-secure digital transformation over the 2021-2027 Multiannual Financial Framework, the EU has the unique opportunity to pool its assets to propel its Industry Strategy and leadership in digital technologies and cybersecurity across the digital supply chain (including data and cloud, next generation processor technologies, ultra-secure connectivity and 6G networks), in line with its values and priorities. |
| **SCOPE** | This axis relates to the security of the digital supply chain. The EU continues to broadening the concept of strategic autonomy in key sectors such as cybersecurity, telecommunication, AI, cloud computing, space, medical assets, among others. The Axis considers the analysis of EU digital technology supply chains to identify specific dependencies for a number of key technologies (e.g. AI, robotics, industrial automation, next generation internet, 6G, edge computing, quantum, cybersecurity etc.) and assess their impact and risk for selected application domains (e.g. telecommunications, transport, energy, health, industry 4.0, government etc.). Topics reviewing risk management methodologies, vulnerability management, incident reporting and threat intelligence are examples of focus areas in this axis. |
| **OBJECTIVES** | * Digital supply chain resilient to cybersecurity incidents. |
| **WHO** |  |
| **TARGETS**  (e.g. through coordination, legislation, funding) | Automating tools support the software industry in meeting improved security goals, ensuring that vulnerabilities are rapidly found and remediated. |

**Comments from SPARTA on the Axis:**

The CAPE program addresses the entire software development lifecycle, including software that may introduce vulnerabilities (libraries, apps in smartphones, etc.) and is not under the direct control of the developer. It produces tools to evaluate the impact of such software vulnerabilities in products.

**TOPICS TABLE FOR THE AXIS: RESILIENCE OF THE DIGITAL SUPPLY CHAIN**

| **TOPIC** | **DESCRIPTION** | **SELF-ASSESSMENT –**  **COMPLETED** | **SELF-ASSESSMENT -**  **ON GOING** | **POSSIBLE WAYS FORWARD** | **ACTORS** |
| --- | --- | --- | --- | --- | --- |
| **APPROACHES TO IMPROVE THE RESILIENCE OF SUPPLY-CHAIN RESILIENCE** | This topic considers the research and development of novel approaches aiming at the improvement of the digital supply chain resilience to cyberattacks. Examples include the development of index, indicators, processes for the overall supply chain performance improvement, etc. | HAII-T Program develops an integrated framework and a toolkit supporting the design, development and verification of security-critical, large-scale distributed II systems. D6.1: Security by design framework for the intelligent infrastructure. D6.3: First release of demonstration.  HAII-T also targets the Operating Systems software directly for IoT devices such as RIOT to directly provide security enhanced OS for IoT D6.2: Security enhanced OS software. | The CAPE program software assessment tools are being experimented to measure the exposure of software to depending libraries and platform vulnerabilities. This could be leveraged for risk evaluation in the software supply chain.  HAII-T framework will be finalised and further demonstrated in D6.4. | Establishing de-facto world standards on supply-chain resilience, including design, validation, and monitoring of new and existing supply-chains. |  |
| **RISK ASSESSMENT AND MITIGATION METHODS** | This topic explores the adoption of risk management practices in the protection of the digital supply chain. For example, the use of systemic risk assessment approaches across the supply-chain and stakeholders. This topic includes processes, activities and tools related to the continuous assessment of cyber risks and threats and consequent mitigation measures. | SAFAIR program lies in conducting a thorough analysis of the threats and risks for AI. SAFAIR provided a threats and risks analysis for AI systems (D7.1). SAFAIR also aims at providing defensive mechanisms and tools to respond to them. (D7.2, D7.4)systems security mechanisms and tools. | SAFAIR D7.5 will be the continuity of D7.4. |  |  |
| **INCIDENT HANDLING AND REPORTING** | This topic explores the idea of implementing processes and/or systems to report incidents. It refers to incidents affecting one or more suppliers across a supply chain or operators of essential services across the same sector, industry, etc. It also relates to how to handle cyber incidents, share threat intelligence and cooperate during an incident. | T-SHARK D4.1, D4.2 same as first axis. | T-SHARK D4.3-6 will address comprehensive threat analysis. |  |  |
| **VULNERABILITY MANAGEMENT** | This topic refers to the need to coordinate the disclosure of vulnerabilities. It also includes the identification of processes related to the coordination of the patching and updating of systems included in a supply-chain or critical infrastructure. | WP2 D2.3 presents a preliminary analysis of common vulnerability disclosure policies in Europe. | Same as above for CAPE  T-Shark D4.3-6 will address this topic as it is an important part of Threat intelligence in relation with WP2 D2.5. |  |  |
| **VENDOR CERTIFICATION** | This topic aims at promoting transparency in the level and type of participation of all the entities involved in the supply chain of a product or service supporting EU critical infrastructure. It discussed the need for an industry certification for digital supply-chain security. |  | CAPE is developing tools that support certification of software. Usage of such tools could lead to vendor certification. | Catalysing the emergence of a certification industry for digital supply-chain security, with world-wide capacities |  |
| **MATURITY ASSESSMENT** | This topic acknowledges the importance of conducting regular maturity assessment of entities maintaining EU critical infrastructure in the level of resilience to cybersecurity incidents and threats. This topic includes the adoption of various techniques such as penetration testing, security testing and threat modelling. |  | D4.3-4 Cybersecurity threat methodology and prediction framework | Link maturity assessment with continuity of supply chain certification. |  |
| **PANDEMIC/CRISIS** | This topic reviews the impact of the current pandemic crises in cybersecurity. It also reflects on the risks associated with supply chains needs during pandemic/crisis situations. | SPARTA Roadmap committee has assessed the implication of COVID-19 on the SPARTA Roadmap in D3.3.  SPARTA Governance has also assessed this impact in D1.3 and with the help of an external assessment in D1.4 on the SPARTA ecosystem. |  |  |  |
| **TRANSPARENCY IN THE SOFTWARE SUPPLY-CHAIN** | This topic refers to improvements in the security of the software supply-chain to promote transparency. It considers the enhancing the level of transparency to reinforce the trust between the various parties and other relevant stakeholders. |  |  |  |  |
| **OPEN SOURCE SOFTWARE AND OPEN DATA** | This topic explores the security impact when using open-source software in critical infrastructure and the digital supply chain. It also includes the research of challenges and opportunities for organisations adhering to open data. |  |  |  |  |
| **OTHER TOPICS** |  |  |  |  |  |

**Additional input on the Axis:**

|  |  |  |  |
| --- | --- | --- | --- |
| **TOPIC** | **DESCRIPTION** | **POSSIBLE WAYS FORWARD** | **ACTORS** |
| **ENHANCING SYNERGIES AND COORDINATION BETWEEN THE CYBERSECURITY CIVILIAN AND DEFENCE SPHERES** | This topic relates to the activities facilitating the exchange of information, results, requirements, priorities of relevant Union programmes in relation to the synergies and coordination developed in the cybersecurity civilian and defence spheres. | D4.3 Comprehensive full-spectrum cybersecurity threat intelligence methodology  Building on, ECCCN can establish pan-EU coordination platform between different interrelated sectors.  Establishing continuously synchronized integrity with related priority industries including SPACE, DEFENSE, CRITICAL INFRASRTUCTURE and other.  Primary focus on end-user centric cybersecurity delivery. |  |

**Comments from SPARTA on the Axis:**

SPARTA has widely experimented with different governance models and management practices focusing on multi-disciplinary aspects of cybersecurity domain, as well multi-national research and innovation development activities. Collaborative and integrity aspects of joint work is most critical for effective process organization EU-wide. It is not enough to bring RTO and other stakeholders round the table to work on common initiative, engagement and enablement followed by well-fitted coordination model is critical for mature results achievement.

Another aspect to be highlighted is timely addressed dynamics of the global domain and minimized latency in required strategic direction alignments. SPARTA governance model progress with practical instruments to establish necessary procedures and concepts, those further can be maturated in the scope of an extended DoA to cover required scope and to validate it.

Synergized and highly synchronized strategic work shows to bring most of work carried out including interlinked domains of Cybersecurity and Defence, Digital Europe, e-Commerce, DIHS.

|  |  |
| --- | --- |
| **AXIS** | **STIMULATION OF THE EU CYBERSECURITY MARKET** |
| **POLICY**  **CONTEXT/**  **AREAS OF**  **EU ACTION** | A reinforced presence on the technology supply chain: With its planned financial support for cyber-secure digital transformation over the 2021-2027 Multiannual Financial Framework, the EU has the unique opportunity to pool its assets to propel its Industry Strategy and leadership in digital technologies and cybersecurity across the digital supply chain (including data and cloud, next-generation of processor technologies, ultra-secure connectivity and 6G networks), in line with its values and priorities. |
| **SCOPE** | An axis related to the initiatives and activities aiming at improving citizen’s trust in digital technology. It focuses on adopting measures that stimulate the European cybersecurity market. Topics under this axis should consider the demand side of the cybersecurity market to consider the aspects of the economics underlying the sustainability of EU implementations of cybersecurity solutions for a wide range of threats and foster the proper segmentation of products and services. |
| **OBJECTIVES** | * Improve citizen’s trust in digital technology. * Increase the offer of EU-based cybersecurity solutions (product and services). |
| **WHO** | * Focus groups on SMEs and start-ups * European cybersecurity cooperation structures, adoptive dynamic approaches and actors |
| **TARGETS**  (e.g. through coordination, legislation, funding) | * EU should target coordination and, above all, full regulatory support for innovative business models for cybersecurity (e.g., encryption and key escrow as a service, intrusion detection as a service, incident management as a service). * Strategic priorities for cybersecurity research, innovation, last-mile development, productization, marketization and uptake * Main Achievements should include:   + Priorities for last-mile development, productization and marketization of selected EU cybersecurity innovations   + Setting up and continuously propagating joint infrastructures for both cybersecurity R&I purposes, and for supporting collaborative work operations (secure communications, secure agendas, etc.) * EU Targets should ensure focused dissemination and facilitated collaboration of research outcomes, innovations, EU-wide cybersecurity strategic communication to reach stronger impact * Mediation for healthy and balanced, strategic priorities driven coopetition among different EU cybersecurity R&I&D actors |

**Comments from SPARTA on the Axis:**

SPARTA establish and develops JCCI (joint cybersecurity competence infrastructure) as sharing and collaboration platform that provides controlled access the individual cybersecurity research outcomes, tolling, innovative solutions. It provides the basis for successful use, (re)use and evolution of current results to meet final users’ needs and to solve last mile development issue.

SPARTA Networking schema and instruments: SPARTA Associates, SPARTA Friends, SPARTA Days, SPARTA Brokerage initiative provides the instrument for community engagement, empowerment and facilitation for new and evolving collaborations in that way stimulating mission focused partnership and SME as Start-ups development. At the same time it works as tipping point for fragmented individual initiatives and creates space for mentored and one mission oriented coopetitive effort.

**TOPICS TABLE FOR THE AXIS: STIMULATION OF THE EU CYBERSECURITY MARKET**

| **TOPIC** | **DESCRIPTION** | **SELF-ASSESSMENT - COMPLETED** | **SELF-ASSESSMENT -**  **ON GOING** | **POSSIBLE WAYS FORWARD** | **ACTORS** |
| --- | --- | --- | --- | --- | --- |
| **SUPPLY AND DEMAND CHALLENGES AND STIMULATION MEASURES** | This topic explores the options and measures required to stimulate the supply and demand of cybersecurity products and services. This topic includes taking stock of the current cybersecurity market in order to understand the different dynamics, trends and players. |  |  |  |  |
| **SMEs** | This topic refers to the research of possible options or innovative ways to attract SMEs into the technology sector and promote entrepreneurship to develop cybersecurity solutions (products and services). It also refers to leveraging the potential of SMEs to operate in the cybersecurity market. |  |  | Focus group on SMEs | Pilots |
| **SCREENING OF FOREIGN DIRECT INVESTMENT** | This topic identifies possible options and innovative ways to attract foreign direct investment in the EU cybersecurity market. |  |  |  |  |
| **SECURITY-BY-DESIGN AND BY-DEFAULT IN DIGITAL PRODUCTS AND SERVICES** | This topic refers to the processes that acknowledge cybersecurity and privacy as essential requirements in product innovation, the production and development processes, including the design phase (security-by-design), throughout a product’s entire life cycle and across its supply chain. | CAPE program addresses assessment of cybersecurity properties for software. Includes a method to jointly specify security and safety properties, what we call security-safety codesign. D5.1: Assessment specifications and roadmap, D5.2. | The CAPE assessment methods and tools are being linked with certification processes, especially incremental certification for continuity of certification with the help of WP11: D5.3 and D5.4. | Stimulate European cyber security products and processes (also with labels/certification) |  |
| **MARKET FACTORS** | This topic explores the key factors that are driving the cybersecurity market. The aim is to find solutions for the challenges and explore the opportunities that the market offers. |  |  |  |  |
| **OTHER TOPICS** |  |  |  |  |  |

|  |  |
| --- | --- |
| **AXIS** | **IMPROVING EU TECHNOLOGICAL SOVEREIGNTY IN CYBERSECURITY** |
| **POLICY**  **CONTEXT/**  **AREAS OF**  **EU ACTION** | Resilience, technological sovereignty and leadership. The upcoming decade is the EU’s opportunity to lead in the development of secure technologies across the whole supply chain. Ensuring resilience and stronger industrial and technology capacities in cybersecurity should mobilise all necessary regulatory, investment and policy instruments. |
| **SCOPE** | An axis focused in improving the EU technological sovereignty in cybersecurity. Topics should focus on involving the industry and academic communities to develop the EU’s technological sovereignty in cybersecurity, building capacity to secure sensitive infrastructures such as 5G, and reduce dependence on other parts of the globe for the most crucial technologies. |
| **OBJECTIVES** | * Reduce the EU dependency from 3rd countries to protect EU digital infrastructure |
| **WHO** | Focus group on this topic? |
| **TARGETS**  (e.g. through coordination, legislation, funding) | * Drive European Cybersecurity Standards' development harmonization, integrity across stakeholders’ groups in EU and ensure actuality in global context * Play an active role in establishment and continues development of strategic alliances beyond EU, representing EU cybersecurity stakeholders’ priorities |

**Comments from SPARTA on the Axis:**

The CAPE program develop tools to deal with vulnerabilities in external software. This could be extended to list software libraries and operating systems that are absolutely required for operating products and services. For example, it is very likely that the TensorFlow library has become a critical resource. If Google were to phase out the library, we would lose this capability.

The key aspect to be considered that sovereignty and strategic autonomy does not provide long lasting results by implementing separation and close market principles. The way forward is balanced politics combining global collaboration, global leadership and trusted diversified partnership.

**TOPICS TABLE FOR THE AXIS: IMPROVING EU TECHNOLOGICAL SOVEREIGNTY IN CYBERSECURITY**

| **TOPIC** | **DESCRIPTION** | **SELF-ASSESSMENT - COMPLETED** | **SELF-ASSESSMENT -**  **ON GOING** | **POSSIBLE WAYS FORWARD** | **ACTORS** |
| --- | --- | --- | --- | --- | --- |
| **PUBLIC AND PRIVATE FUNDING** | This topic refers to the research of possible options or innovative ways to attract public and private funding investment in cybersecurity projects in the EU market and compete globally. It also includes the development of public-private partnerships. |  |  |  |  |
| **INCUBATORS AND ACCELERATORS** | This topic refers to the requirement to incubate and accelerate cybersecurity projects. It relates to concepts around supportive and community-oriented programmes, including events and access to mentoring, coaching and entrepreneurial networks. It also includes developing targeted programs and services offered to early-stage companies to help them refine their product offering and accelerate their business. |  |  |  |  |
| **BUSINESS MODELLING** | This topic considers the development of innovative business/marketing strategies to increase EU companies' competitiveness in the Union and the global cybersecurity market. New ideas on how to stimulate the transition of research projects into innovative businesses. |  |  |  |  |
| **VENTURE CAPITAL** | This topic focuses on researching innovative ways to attract venture capital to invest in EU cybersecurity projects. It considers working with start-ups and small businesses that are believed to have long-term growth potential to make them visible and attractive to VC firms. |  |  | Create European venture capital companies (possibly state supported) |  |
| **SIMPLIFY PROCUREMENT PROCEDURES** | This topic aims to explore and develop simplified procurement procedures (with a clause of “Digital Sovereignty”) to strengthen the European IT industry. |  |  | Add labels for improving the positioning of European companies |  |
| **DEPENDENCY FROM NON-EU IT/ CYBERSECURITY PRODUCTS** | This topic aims at identifying priority areas, promoting and reducing the EU dependency from Non-European IT products supporting the EU critical infrastructure. It also considers increasing redundancy and multi-sourcing. Identifying critical dependencies, mitigating the risk from incorporating essential components, having redundancy and multi-sourcing strategies. | The SPARTA Roadmap identifies priority areas, starting from the 4 Programs and expanding as it iterates (D3.1, D3.2) | D3.3 is ongoing, and will benefit from cross-pilot discussions | Sustain continuous roadmapping efforts throughout the Digital Decade, leveraging community feedback | SPARTA’s Roadmap Committee |
| **OTHER TOPICS** |  |  |  |  |  |

|  |  |
| --- | --- |
| **AXIS** | **HUMAN AND SOCIAL PERSPECTIVE** |
| **POLICY**  **CONTEXT/**  **AREAS OF**  **EU ACTION** | The EU should continue to work with international partners to promote a political model and vision of cyberspace grounded in the rule-of-law, human rights, fundamental freedoms and democratic values that bring social, economic and political development globally and contribute to a Security Union. |
| **SCOPE** | This axis focuses on non-technological aspects and how technology is used, perceived, and promotes change in society. This axis includes essential elements such as inclusiveness, trustworthiness, fairness and ethics in the use of digital technology. The aspect of ‘European values’ includes freedom, equality, democracy, and data protection by adding human rights, democratic principles, and the rule of law. |
| **OBJECTIVES** | * Protect EU values in the digital space; |
| **WHO** | Focus group on privacy and ethics |
| **TARGETS**  (e.g. through coordination, legislation, funding) | * Quarterly or bi-yearly workshop events gathering project performers on human and social perspectives * Creation of an Digital Ethics Commission, tasked with mapping MS-level initiatives, and animating EU-level interactions * Development and publication of European doctrines on Openness and transparency, Liability and Accountability, etc. (see Joint taskforces, see 6) * A funding objective of 30% of research projects including a demonstrable multi-disciplinary consortium and work plan (tamping up over the 3 first years of FP9). * Special focus on identification and adopted measures to higher cyber vulnerability societal groups, incl. elderly and children. * Identification and definition of known unregulated grey zones followed by continues improved security policies, regulation, standards and measures considering improvements in industry developments as well consumer behaviour |

**Comments from SPARTA on the Axis:**

While developing and implementing equality and freedom driven policies it should not be forgotten that EU will always be facing societally and technologically vulnerable groups demanding for special attention and attitude (elderly groups, children, remote and other limited capabilities regions). We should secure minimum cybersecurity standard for all EU society. This minimum cybersecurity standard must be defined, implemented and constantly improved to secure overall EU digital ecosystem evolution in that way preparing the society for early-stage large scale innovations adoption and exploitation including AI, Quantum, Bio-tech, 6G.

General awareness and scientific evidence-based acceptance of future technologies, low fear level of technology driven disruptive changes as well opportunities understanding combined with well-timed regulatory and policy developments are the key for success.

Constant review and identification of changing environment while identifying trending and newly appearing unregulated grey-zones should be organized in coordinated manner involving all MS and represented by all types of societal groups.

**Possible addition to the targets:**

\* Does the last target mean, that 30% of projects shall have a multi-disciplinary consortium? That’s a weak target. I would suggest to ask that \_each\_ project should address issues beyond the purely technical ones.

\* It would be nice if there were distinct projects addressing fundamental multidisciplinary issues (like CANVAS) but it’s even more important to have an “embedded social/legal/ethical scientist” in each tech oriented project as well.

In the following table: many of the aspects cannot be treated separately (openness, fairness, inclusiveness etc.) are part of a necessary holistic treatment of human and social aspects

**TOPICS TABLE FOR THE AXIS: HUMAN AND SOCIAL PERSPECTIVE**

| **TOPIC** | **DESCRIPTION** | **SELF-ASSESSMENT - COMPLETED** | **SELF-ASSESSMENT -**  **ON GOING** | **POSSIBLE WAYS FORWARD** | **ACTORS** |
| --- | --- | --- | --- | --- | --- |
| **ETHICS** | This topic explores different research options and presents solutions for the ethical part in technology and the interplay with cybersecurity. | WP 2 has given general guidance on ethical issues and approaches (D2.1, D2.2) | WP 2 is developing method to assess and improve “societal readiness” from an early development phase on and will deliver general guidelines on this (D2.6) | Cementing the EU leadership in ethical cybersecurity and informatics.  Creating a world-leading expertise in human and social sciences for cybersecurity. |  |
| **PRIVACY** | This topic focuses on security and privacy concerns related to the collection and handling of personal data. It relates to the research of different aspects of privacy, including data anonymisation, privacy-by-design, data privacy, and privacy protection techniques. | WP 2 has given general guidance on privacy requirements. (D2.1, D2.2) | In addition of general guidelines (D2.6). Programmes have partners addressing specific privacy issues of the solutions under development which will be reported in D2.5 and in some program deliverables (D7.1, D7.3, …). |  |  |
| **IDENTITY MANAGEMENT** | This topic considers the research of digital identity as a human, social aspect and organizational process for ensuring that individuals have the appropriate access to technology resources. More specifically, this topic includes the identification, authentication and authorization of a person, or persons, to have access to applications, systems or networks. It includes trust management, authentication, authorisation and interoperability. |  |  |  |  |
| **LIABILITY AND ACCOUNTABILITY** | This topic identifies the challenges and explores the options to deal with the liability and accountability of security issues in technology including software, systems, services, etc. |  |  |  |  |
| **OPENNESS AND TRANSPARENCY** | This topic focuses on novel approaches to improve openness and transparency in the use, exchange and portability of personal data. |  |  |  |  |
| **FAIRNESS AND INCLUSIVENESS** | This topic focuses on the promotion of fairness and inclusiveness in the use of the digital space. It explores the need for Europe to become more inclusive, open, fair, diverse, democratic, confident and encourage women to take part fully. | Best-practice guide on how to attract and retain women in cybersecurity teams – A communication effort  Fairness is also being addressed in the context of the SAFAIR program with regards to machine learning methods and how to promote and help the development of fair AI tools. (D7.1-2-4) | Engagement of some outermost regions on the research program and deliver cybersecurity training and awareness workshops.  SAFAIR (D7.5) |  |  |
| **USER ASPECTS** | This topic focuses on the research of the different roles of human interaction with technology such as user, consumer, patient (healthcare), administrator (systems), passenger (transport), student (education), the data subject (identity) or simply a citizen (government), etc. |  | D4.5 Cybersecurity threat prediction legal framework, | Complement system-security perspective (target: organisational users; network operators; service providers) to security solutions to empower citizens (increase citizens' sovereignty in dealing with data and systems) |  |
| **TRUST IN DIGITAL SOLUTIONS** | This topic explores new approaches to improve citizens trust in digital solutions. It considers aspects such as transparency and accessibility to information about digital business practices, protecting user preferences on the use of personal data, among others. | SAFAIR is addressing topics of personal data protection in AI system and how to build trustworthy AI. (D7.1-2-4) | SAFAIR D7.5 |  |  |
| **USER RESILIENCE** | This topic focuses on improving individual’s resilience to cyberattacks. It includes new strategies to help citizens adopting proactive measure to recover from a cyberattack. |  |  |  |  |
| **USER AWARENESS** | This topic focuses on developing innovative ways of improving user awareness concerning cybersecurity and privacy. This topic aims at developing new processes that seek to inform and educate people about cybersecurity to influence their attitudes, behaviours, and beliefs towards achieving a defined purpose or goal. |  |  |  |  |
| **eIDAS-BASED TRUST FRAMEWORK** | This topic identifies different options to coordinate, legislate and fund a common eIDAS-based trust framework for Member State digital identity trust schemes. |  |  |  |  |
| **OTHER TOPICS** |  |  |  |  |  |

|  |  |
| --- | --- |
| **AXIS** | **CYBERSECURITY AWARENESS** |
| **POLICY**  **CONTEXT/**  **AREAS OF**  **EU ACTION** | A cyber-skilled workforce. The Revised Digital Education Action Plan will raise cybersecurity awareness among individuals, especially children and young people, and organisations, especially SMEs. |
| **SCOPE** | This axis focuses on topics related with improving citizen awareness on cybersecurity risks. It considers the development of awareness tools and guidance to increase the resilience of EU citizens, businesses and organisations against cyber-threats. |
| **OBJECTIVES** | * Increase citizen’s awareness on cyber threats. * Increase CEOs awareness |
| **WHO** |  |
| **TARGETS**  (e.g. through coordination, legislation, funding) | * Large-scale awareness campaigns including EU’s outermost regions, on high-schools, SMEs, social media, specific media such as EU’s cybersecurity and digital privacy newsletter, ECSO, CYBERWISER, etc. * Alignment of awareness campaigns with the EU CSF. * Integration of specific focus groups, such as elderly people, children, people with specific needs, SMEs. * European cybersecurity cooperation structures, adoptive dynamic approaches and actors * Drive European Cybersecurity Standards' development harmonization, integrity across stakeholders groups in EU and ensure actuality in global context |

**Comments from SPARTA on the Axis:**

This must be done in close coordination with the "human and social aspects" – only if human aspects are seriously taken into account raising awareness is reasonable. Otherwise measures to gain acceptance is “ethics washing” and will be counterproductive.

**TOPICS TABLE FOR THE AXIS: CYBERSECURITY AWARENESS**

| **TOPIC** | **DESCRIPTION** | **SELF-ASSESSMENT - COMPLETED** | **SELF-ASSESSMENT -**  **ON GOING** | **POSSIBLE WAYS FORWARD** | **ACTORS** |
| --- | --- | --- | --- | --- | --- |
| **USER AWARENESS** | This topic focuses on developing innovative ways of improving user awareness concerning cybersecurity and privacy. This topic aims at developing new processes that seek to inform and educate people about cybersecurity to influence their attitudes, behaviours, and beliefs towards achieving a defined purpose or goal. | Strategies for the creation of cybersecurity awareness campaigns.  SAFAIR AI Contest (D7.3) | Workshops, lectures, talks, meetings for cybersecurity awareness.  D4.6 Visual Analytics System for Cybersecurity threat analysis  SAFAIR AI Contest (D7.6) | Events for specific groups, such as children, elderly, people with specific needs, etc. | Pilots |
| **~~TRAINING~~** | ~~This topic focuses on researching options and innovative ways to improve cybersecurity training from both the demand and supply sides.~~ | ~~Development of practical software tools that apply the EU Skills Framework and help educational institutions to build cybersecurity curricula in practice. Creation of training scenarios.~~ |  |  |  |
| **COMMUNICATION & dissemination** | This topic reviews the outreach and dissemination of capacity building and training activities. | Strategies for cybersecurity communication & dissemination  Cybersecurity awareness campaigns on social media.  Toolkit with cyber hygiene measures to SME  Scientific dissemination activities (conference papers – journals)  Monthly workshops and other events | Communication & disseminations campaigns for various target groups, such as high-schools and SMEs.  Cybersecurity training workshop on three Outermost Regions | Focusing communication & dissemination on achievements & results while promoting target groups engagement . |  |
| **OTHER TOPICS** |  |  |  |  |  |

|  |  |
| --- | --- |
| **AXIS** | **CAPACITY BUILDING (DEMAND AND SUPPLY)** |
| **POLICY**  **CONTEXT/**  **AREAS OF**  **EU ACTION** | **A Cyber-skilled EU workforce:** The EU’s efforts to upskill the workforce, to develop, attract and retain the best cybersecurity talent and to invest in world-class research and innovation form an important component of protecting against cyber threats generally. |
| **SCOPE** | This axis focuses on the topics related with the development of skills in cybersecurity from both the demand and supply side. It explores the options on how to improve education and training in cybersecurity by identifying the needs of the recipient and the provider. |
| **OBJECTIVES** | * Raise the number of high-quality higher-education study programs on cybersecurity * Raise the number of high-quality professional trainings on cybersecurity * Raise the number of well-trained cybersecurity professionals. * Connect industry and training providers, provide universal skills framework defining terminology and definitions of knowledge, skills and work roles in cybersecurity. |
| **WHO** | Focus group on cyber ranges and education  Focus group on competence centre cyber infrastructure |
| **TARGETS**  (e.g. through coordination, legislation, funding) | * Agreement on EU-wide Cybersecurity Skills Framework (EU CSF). * Development of practical software tools that apply the EU Skills Framework and help educational institutions to build cybersecurity curricula in practice.... * Deployment of larger pilots for cybersecurity study programs and support of education providers in creating new cybersecurity study programs using the EU CSF. * Creation and first deployment of open-source cyber range tools.... * Pilots for open-source cyber-range infrastructures at universities. * Full-fledged open-source cyber ranges for higher-education institutions that cannot adopt commercial products due to costs and closed environment.... * Creation of training scenarios.... * Production of practical tools supporting creation of new training scenarios at users’ premises.... * Ecosystem for sharing free training scenarios among different infrastructures.... * Consolidation of the cyber range domain.... * Creation of domain-specific cyber range infrastructures, e.g. for critical infrastructures, industrial networks, IoT, etc. * Distant learning curricula designed using lessons learnt during COVID time.... * Production of tools for distant learning support, including remotely accessible cyber ranges. * Support continuous education and specialized courses for specific groups, such as kids, elderly people, persons with specific needs. |

**Comments from SPARTA on the Axis:**

SPARTA adopted a complex cybersecurity skills framework based on standardized definitions that helps with the identification of skills and knowledge necessary for cybersecurity work positions. Furthermore, we practically implement the framework in the form of an interactive web application for cybersecurity curricula design. The app, called Curricula Designer, is built upon the framework and allows intuitive design of higher education curricula and their analysis with respect to requirements of work roles already defined in widely-accepted standards. Using the analytical functions, it is easy to identify missing content in the courses and precisely structure the study program so that the graduates are well-prepared to enter the job market.

It should evolve into constant structure and ecosystem addressing dynamics of cybersecurity domain and should adopt to identified, recognized and commonly agreed capability frameworks.

**TOPICS TABLE FOR THE AXIS: CAPACITY BUILDING (DEMAND AND SUPPLY)**

| **TOPIC** | **DESCRIPTION** | **SELF-ASSESSMENT - COMPLETED** | **SELF-ASSESSMENT -**  **ON GOING** | **POSSIBLE WAYS FORWARD** | **ACTORS** |
| --- | --- | --- | --- | --- | --- |
| **TRAINING AND EDUCATION** | This topic focuses on researching options and innovative ways to improve cybersecurity training from both the demand and supply sides. | SPARTA D9.1: Cybersecurity skills framework  SPARTA D9.2: Good-practice curricula descriptions  SPARTA D9.3: Training Evaluation Pilot | Development of practical software tools that apply the Skills Frameworks and help educational institutions to build cybersecurity curricula in practice. | Support EU Cybersecurity Skills Framework, when ready, by a set of practical tools and guidelines.  Creation of large-scale training pilots.  Design good practices for training and education curricula for specific groups, such as critical infrastructures, CBRN, etc.  Develop tools and methods for using EU CSF for curricula design and their evaluation, eventually the certification of cybersecurity study programs and professional trainings. | Pilots |
| **CYBER RANGES** | This topic discusses the design and development of cyber ranges as a cybersecurity research infrastructure for specific technologies, sectors and contexts. It also considers the implementation of Cyber Ranges to provide a multipurpose virtual environment to organisations, sectors, industries, etc. | SPARTA D9.4: Pilot of Cyber training & exercise Framework  Partial coordination among cyber range providers.  Partial technological compatibility, first open-source cyber range tested. | Creation and first deployment of open-source cyber range tools, pilots for open-source cyber-range infrastructures at universities. | Creation of ecosystem for designing and sharing training scenarios.  Developing sustainability model for maintaining cyber range tools and scenarios. | Pilots |
| **EXERCISES** | This topic focuses on novel approaches to structure cybersecurity exercises. It relates to designing innovative ways to develop simulations and attack scenarios custom-tailored for specific sectors, industries and organisations. | As described above – cyber ranges. | As described above – cyber ranges. | As described above – cyber ranges.  Disseminate, maintain and support open-source cyber ranges for use in academia and SMEs. | Pilots |
| **CAPACITY BUILDING** | This topic relates to the research and development of options and innovative ways of building capacity in cybersecurity. The aim is for individuals and organizations to obtain, improve, and retain the skills, knowledge, tools, equipment, and other resources needed to do their jobs competently. | Already covered in Training and Education JCCI – Deliverables 8.1 and 8.2 for the set of tools for the SPARTA JCCI | Already covered in Training and Education Working on D8.3 for JCCI | Already covered in Training and Education | Pilots |
| **TESTING LABS** | This topic discusses the implementation of testing labs as a cybersecurity research infrastructure. These infrastructures will enable the conduction of experiments with known measurements in a controlled environment. The aim is to mimic live production environments as closely as possible. | SPARTA D9.4: Pilot of Cyber training & exercise Framework  Development of training infrastructures for hands-on training at partners of SPARTA involved in cyber range activities. | Development of training infrastructures for hands-on training at more partners of SPARTA. | Interoperability and connection of training labs among multiple partners, across pilots. Develop an open source tool chain to benchmark products and guarantee a minimum level of cyber protection. The tool chain can be offered as a services | Pilots |
| **UPSKILLING AND RESKILLING** | This topic focuses on upskill training, long-life learning and reskilling in cybersecurity competencies. It considers the development of new techniques to train users who have shown they have the aptitude for learning a completely new occupation or providing training to those who need to learn new skills to improve their current performance. | **-** | **-** | Integration of upskilling and reskilling activities with running education and training activities. | Pilots |
| **OTHER TOPICS** |  |  |  |  |  |
| **Tool chain for security by design (JCCI)** | This topic focuses on creating a set of tool and methodologies for the secure design of products and services. This is the design counterpart of the cyber ranges topics that focuses more on the execution part. |  |  | JCCI could/should be integrated with other Pilots infrastructure to avoid fragmentation. The current decentralized structure of JCCI could ease such process. |  |

|  |  |
| --- | --- |
| **AXIS** | **STRATEGIC PRIORITIES FOR CYBERSECURITY RESEARCH, INNOVATION AND UPTAKE** |
| **POLICY**  **CONTEXT/**  **AREAS OF**  **EU ACTION** | Cybersecurity is a priority also reflected in the EU's next long-term budget (2021-2027). Under the Digital Europe Programme the EU will support cybersecurity research, innovation and infrastructure, cyber defence, and the EU's cybersecurity industry. |
| **SCOPE** | Setting a common EU cybersecurity research roadmap will improve the Union's Digital Infrastructure's resilience, reduce the dependency on 3rd countries technology to protect its critical infrastructure and improve the Union's ability to compete in the global cybersecurity market. This topic discusses the process to define a common EU cybersecurity research and innovation roadmap and identify the options to improve its uptake. |
| **OBJECTIVES** | * Reduce the dependency from non-EU cybersecurity technology; * Increase cybersecurity innovation; |
| **WHO** | Focus group on road maps |
| **TARGETS**  (e.g. through  coordination,  legislation, funding) | An **evergreen call for contributions**, leveraging an online infrastructure, with a well-defined scope and structure for inputs  The constitution of a **scientific committee** in charge of coordinating contributions and synthesizing them coherently.  A **continuously-updated strategic priority document**, with (bi-)yearly releases |

**Comments from SPARTA on the Axis:**

While successfully developing EU level strategic priorities and roadmaps for success it is crucial to ensure well organized transfer and adoption of these strategies into MS level as well relevant stakeholders’ groups.

**TOPICS TABLE FOR THE AXIS: STRATEGIC PRIORITIES FOR CYBERSECURITY RESEARCH, INNOVATION AND UPTAKE**

| **TOPIC** | **DESCRIPTION** | SELF-ASSESSMENT - COMPLETED | **SELF-ASSESSMENT -**  **ON GOING** | **POSSIBLE WAYS FORWARD** | **ACTORS** |
| --- | --- | --- | --- | --- | --- |
| **TECHNOLOGY PRIORITIES (AI, CRYPTOGRAPHY, QUANTUM, BIO TECHNOLOGY, ETC).** | This topic focuses on the research of security options and requirements for emerging technologies. It includes conducting foresight activities to identify emerging trends on economic, societal and political change with the adoption of emerging technologies. More specifically, emerging change with a significant impact on the security of the digital space. | SPARTA Roadmap (D3.\*) | 4P SRIAs: high-level meta-roadmap guideline featuring common and individual 4P views on future SRI, with forward references to the detailed pilots' roadmaps.  Setting up a 4P SRIAs consolidation event: present each pilot's priorities for cybersecurity SRI in Europe |  |  |
| **VERTICAL APPLICATION AREAS (HEALTH, TRANSPORT, FINANCE, ETC).** | This topic focuses on the research and development of innovative solutions, security options and requirements for specific vertical areas such as health, transport, finance, utilities, logistics, manufacturing, etc. | SPARTA Roadmap (D3.\*) |  |  |  |
| **RESEARCH INFRASTRUCTURE** | This topic explores the requirements to implement cybersecurity research infrastructures—the availability of research infrastructure to support the testing cybersecurity solutions. | SPARTA D8.1 and D8.2 for JCCI. |  | Merge the tool chains of the 4P |  |
| **OPEN SOURCE** | This topic considers the exploration of research opportunities to develop open-source security software solutions, open-source service providers (e.g. cloud, edge), among other options. |  |  |  |  |
| **PROTECTION OF INTELLECTUAL PROPERTY** | This topic explores innovative ways of protecting intellectual property. It considers creative ways to prevent the theft or copy of names of products, brands, inventions, design or look of products, authorship, copyright, patents, design, trademarks or any other types of intellectual property. |  |  |  |  |
| **INNOVATION** | This topic focuses on the promotion of innovation in cybersecurity and more specifically, on how research projects may transition into development and ultimately into new products/services. |  | T-Shark is experimenting and developing cross-broader, multi-project, multi-solution innovation governance model |  |  |
| **OTHER TOPICS** |  |  |  |  |  |

|  |  |
| --- | --- |
| **AXIS** | **EUROPEAN CYBERSECURITY COOPERATION STRUCTURES, APPROACHES AND ACTORS** |
| **POLICY**  **CONTEXT/**  **AREAS OF**  **EU ACTION** | The EU aims, through the full implementation of regulatory tools, mobilisation and cooperation, to support Member States in defending their citizens, as well as their economic and national security interests, in full respect of fundamental rights and freedoms and the rule of law. |
| **SCOPE** | This axis highlights the importance of fostering cooperation and aligning approaches between different EU cybersecurity actors to achieve results. Cooperation and coordination will be required to reducing cybersecurity threats and improving resilience to cybersecurity incidents. |
| **OBJECTIVES** | * Promote cooperation between different EU actors and with international organisations. |
| **WHO** | Focus group on community lead and governance  (split in two groups one for community and the other for governance??) |
| **TARGETS**  (e.g. through  coordination,  legislation, funding) | * Establishing joint taskforces across structures, ranging over the 3 pillars of cybersecurity: cybercrime, cyberdefense, and information systems security * Establishing a Joint Strategic Oversight Committee, continuously evaluating the activities of taskforces, spinning up new taskforces with clear mandates, and shutting down obsolete ones * Mapping out clear and efficient liaison contact points across various structures, with a special focus on regional contact points. |

**Comments from SPARTA on the Axis:**

SPARTA Networking schema and instruments: SPARTA Associates, SPARTA Friends, SPARTA Days, SPARTA Brokerage initiative provides the instrument for community engagement, empowerment and facilitation for new and evolving collaborations in that way stimulating mission focused partnership.

**TOPICS TABLE FOR THE AXIS: EUROPEAN CYBERSECURITY COOPERATION STRUCTURES, APPROACHES AND ACTORS**

| **TOPIC** | **DESCRIPTION** | **SELF-ASSESSMENT –**  **COMPLETED** | **SELF-ASSESSMENT -**  **ON GOING** | **POSSIBLE WAYS FORWARD** | **ACTORS** |
| --- | --- | --- | --- | --- | --- |
| **INCENTIVES FOR COMMUNITY PARTICIPATION** | What functions should the Community fulfil in order to be advantageous for the different types of stakeholders (as listed in article 8 of the draft Regulation): Outreach, specialised sub-communities, capacity-sharing, input to policy/public funding…? | * Publishing elements of European doctrines * Conducting joint prospective exercises, scoping out future cyber-pandemics and geostrategic disruptions * Conducting joint crisis exercises |  |  |  |
| **LESSONS LEARNED CONCERNING ORGANISING THE COMMUNITY** | What should be guiding principles? Roles? Experiences /what worked well? what did not? | D8.1 SPARTA started with a concept of tier community with partners and associates. This idea could be further extended with tier of trust/commitment/engagement.  It turned out to be a good idea in order to have flexibility and another tier of friends was created for those partners mainly interested to receive information prior others. |  | Considering different tiers of engagement (with several criteria).  Achieving diversity and attracting several communities, including end-users (with specific roles) |  |
| **STRUCTURING THE COMMUNITY** | What would be appropriate topics for working groups?  [For comparison: ECSO working groups; 4 pilot work packages] | Along the 9 axis (possibly merging some axis). |  |  |  |
| **COMMUNITY MEMBERSHIP** | How could the general criteria for membership, which are contained in the draft regulation, be "operationalised"? |  |  | Considering several levels of membership (with different benefits/duties). |  |
| **COMMUNITY BUILDING AT NATIONAL VS EU LEVEL** | What structures and activities should rather take place at EU level? Which at national level? [also: regional] | SPARTA approach in D8.1 and D8.2 was about to create at national level strong cluster of partners ranging from academia, government, industry and end users. |  | Matchmaking events to help to know each others at regional/national and EU level. Brokerage event to improve synergies. |  |
| **NATIONAL COORDINATION CENTRES** | What could be an appropriate "service catalogue" for National Coordination Centres?  Other considerations | Matching national demand offer of cyber security services/products/skills.  Easing the uptake of cyber security solutions at national level. |  | Mobilize the national community and network with the other countries |  |
| **ATLAS** | How should it further evolve? What should be information to feature on the atlas? How can the Community contribute to it? |  |  | ATLAS should be able to describe for any topic in the JCR the potential researchers, groups, organizations, tools, products available. |  |
| **COMMUNITY INTERACTIONS** | Role of/links with Digital Innovation Hubs (all DIHs versus DIHs specialised in cybersecurity).  The role of/links with regional governments  What would be other important actors (stakeholder formations; policy structures, international forums…) for the Community to take into account? How should interactions take place? |  |  | Cyber security must be served by a specific EDIH as well as being present as task activity in all the other DIH.  We should avoid however that the cyber security in the different DIH is done separately and thus the European specific DIH in cyber must coordinate / correlate such activities.  Cyber security must be clearly present and identifiable in one place (existence) and available everywhere (presence). |  |
| **ECCC JOINT ACTIONS** | Apart from the formal framework provided by the Regulation, how can the Community activities lead to concrete joint investment by the Union, individual/groups of Member States, and industries?  Any examples? | Public private partnerships should be fostered.  Civil society should be also involved. |  |  |  |
| **OTHER TOPICS** |  |  |  |  |  |