EUROPEAN UNION AGENCY
FOR CYBERSECURITY

PROPOSALS FOR THE EUROPEAN CYBERSECURITY COMPETENCE CENTRE (DRAFT)

OCTOBER 2021

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

For contacting the authors please use info@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

CONTRIBUTORS

European Commission (DG-CNECT), ENISA, CONCORDIA, ECHO, SPARTA, CyberSec4Europe and European Cyber Security Organisation (ECSO).

LEGAL NOTICE

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 2019/881. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time. Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

TABLE OF CONTENTS

1. INTRODUCTION

The European Union Agency for Cybersecurity (ENISA) has a mandate to undertake all tasks necessary to achieve the overall high level of cybersecurity across the Union, which also includes providing advice to EU institutions, bodies, offices and agencies and the Member States on research needs and priorities in the field of Cybersecurity (article 11(1) of the Cybersecurity Act[1]).

In order to fulfil this role, ENISA has first gathered inputs from members of the European Cyber Competence Network[2] on potential areas of focus in cybersecurity research and innovation, and then analysed these on the basis of its expertise and knowledge in the field, to advise on potential priorities, thus contributing to the work of the European Cybersecurity Industrial, Technology and Research Competence Centre and Network (CCCN) in preparation of its Strategic Agenda and Multiannual Work Programme[3].

The CCCN should be the Union's main strategic instrument to pool investment in cybersecurity research and technology deployment, thus contributing to industrial development. The implementation of relevant projects and initiatives will be performed together with the Network of National Coordination Centres and the Competence Community formed by academia, Industry, researchers and cybersecurity professionals.

The CCCN regulation outlines the role of the Competence Community and the importance of benefiting from the experience and the broad representation of relevant stakeholders such as European Cyber Security Organisation (ECSO)[4] and the four Pilot Projects launched in early 2019 under Horizon 2020[5], namely CONCORDIA[6], ECHO[7], SPARTA[8] and CyberSec4Europe[9].

[1] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act, last accessed June 2021.
[2] https://cybercompetencenetwork.eu/, last accessed June 2021.
[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0887&qid=1623142941122, last accessed June 2021.
[4] https://ecs-org.eu/, last accessed June 2021.
[5] https://ec.europa.eu/programmes/horizon2020/en/home, last accessed June 2021.
[6] https://www.concordia-h2020.eu/, last accessed June 2021.
[7] https://echonetwork.eu/, last accessed June 2021.
[8] https://www.sparta.eu/, last accessed June 2021.
[9] https://cybersec4europe.eu/, last accessed June 2021.

OBJECTIVE: The aim of this document is to identify areas of focus for initiatives and activities to be considered in future calls for proposals organised by the ECCC.

The CCCN is composed by the European Cybersecurity Competence Centre (ECCC), Network of National Coordination Centres (NCC) and the Competence Community.

The ECCC mandate include:

- The management of funds foreseen for cybersecurity under Digital Europe and Horizon Europe Programmes 2021-2027.
- Facilitate and help coordinate the Network and Community to drive the cybersecurity technology agenda.
- Support joint investment by the EU, Member States and industry and support deployment of products and solutions.

The NCC:

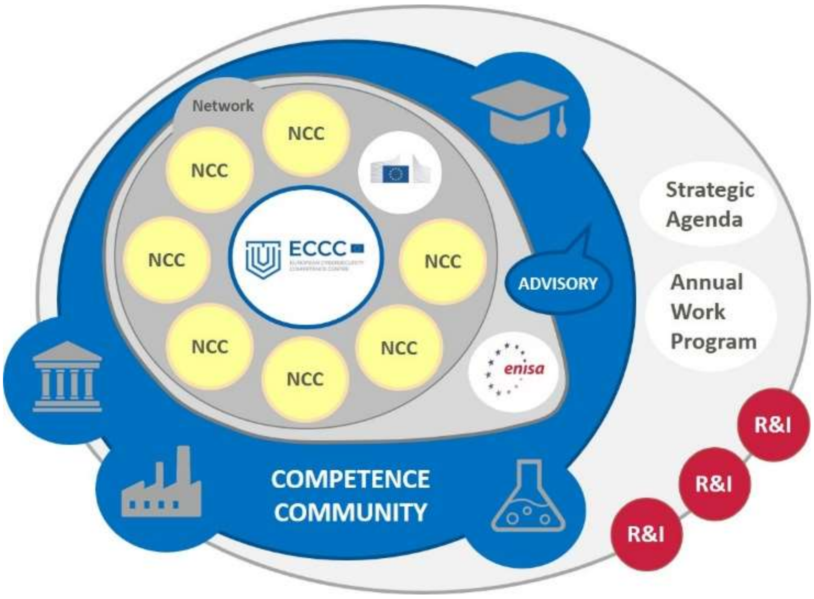
- Will be nominated by Member States as the national contact point.
- Will stimulate national capacity building and link with existing initiatives.

The Competence Community is:

- A large, open, and diverse group of cybersecurity stakeholders from research and the private and public sectors, including both civilian and defence sectors.

The figure below depicts the role of the various entities involved in the CCCN.

Figure 1 - Entities involved in the CCCN



1.1 THE ENTITIES AND THE COMPETENCE COMMUNITY

The Entities CONCORDIA, ECHO, SPARTA and CyberSec4Europe are the four winning Pilot Projects launched in early 2019 from the Horizon 2020 cybersecurity call[10] establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap.

The mission and objectives of the four Pilot Projects are in line with the idea behind the EC proposal for a European Regulation establishing a European Cybersecurity Industrial, Technology and Research Competence Centre and a Network of National Cybersecurity Coordination Centres.

These Pilot Projects bring together more than 160 partners, including big companies, SMEs, universities and cybersecurity research institutes, from 26 EU Member States. The overall EU investment in these projects will be more than 63.5 million Euros. These Entities were selected among 12 eligible proposals that the EC has received for the Horizon 2020 call.

Finally, in 2016, the EC established contractual public-private partnership (cPPP) on cybersecurity under Horizon 2020 (H2020) with an association consisting of

[10] https://digital-strategy.ec.europa.eu/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network, last accessed June 2021.

members from cyber industry, academia, public administrations and more named European Cyber Security Organisation (ECSO).

The four H2020 Pilot Projects

CONCORDIA

CONCORDIA is an EU-funded multi-disciplinary research and innovation project, set out to address the current fragmentation of the cybersecurity market and further enhance the EU's digital sovereignty. The project aims to interconnect all of Europe’s cybersecurity capabilities into a network of expertise to help build a secure, trusted, resilient and competitive ecosystem. LINK to the website. The end date of the funding is December 31, 2022.

ECHO

The project ECHO aims to deliver an organised and coordinated approach to improve proactive cyber defence of the European Union, allowing the bloc to act in anticipation, defending against an attack on computers and networks. ECHO is developing a network through which the EU Cybersecurity and Competence Centres can be best coordinated and optimised. LINK to the website. The end date of the funding is January 31, 2023.

SPARTA

The digital era has brought with it many advantages for humanity, but the issue of secure data exchange remains among the most significant concerns. The project aims to set up unique collaborations, build transformative capabilities and form world-leading expertise centres. Through innovative governance, ambitious demonstration cases and active community engagement, SPARTA intends to re-think the way cybersecurity research is performed in Europe across various domains and fields of expertise. LINK to the website. The end date of the funding is January 31, 2022.

CyberSec4Europe

Faced with ever-increasing cybersecurity challenges, the European Union is committed to improving its awareness and response to cyber-attacks aimed at Member States or its institutions. CyberSec4Europe aims to boost defences within the vertical sectors of digital infrastructure, finance, government, transport, health and smart cities. The project will utilise practical experience gained during the course of CyberSec4Europe to develop a specialised roadmap and recommendations for the implementation of network competence centres. LINK to the website. The project end date is July 31, 2022.

ECSO	The European Cyber Security Organisation (ECSO) is a Public-Private Partnership established by the EC. ECSO federates the European Cybersecurity public and private stakeholders, including large companies, SMEs and start-ups, research centres, universities, end-users and operators of essential services, clusters and association, as well as the local, regional and national public administrations across the European Union (EU) Members States, the European Free Trade Association (EFTA) and H2020 Programme associated countries. LINK to the website.

1.2 THE PROCESS

To gather the information used in this study, the European Commission (DG-CNECT)[11], with the support of ENISA, asked the Entities to identify past, ongoing and future activities in key areas to improve the Union cybersecurity. The process began with taking stock of the work done using ‘gap analysis’ to identify the degree of coverage in these key areas.

ENISA produced an initial list with 482 inputs received on ‘past and ongoing activities’ and another list with 219 inputs for the ‘way forward’. Both lists contained a wide variety of inputs with different levels of detail, complexity and alignment with the Competence Centre mandate. On ‘past and ongoing activities’, ENISA prepared a separate study and gap analysis and produced four main recommendations, which are presented in Annex 1 and reference throughout this document.

Regarding the ‘way forward’, the original data was classified and grouped by trends, scope and objectives resulting in a shorter list of 59 entries presented in Annex 2 of this document. Additionally to this list, the Entities also provided a consolidated cybersecurity agenda with research challenges of high-priority from the work produced by their road-mapping Focus Group[12]. Based on this data and information, ENISA produced an analysis and also contributed with its own views and ideas on the needs and priorities[13].

An important aspect taken into account was the avoidance of overlap with ENISA’s activities as stated in article 5 (2)(b) of the ECCC Regulation. To strengthen this perquisite, several references were made on how ENISA and other EU bodies can cooperate and collaborate with the ECCC to avoid any duplication of effort.

[11] https://digital-strategy.ec.europa.eu/en last accessed July 2021.
[12] The elements from this agenda are reflected in proposal 2.5.
[13] https://www.enisa.europa.eu/publications/cybersecurity-research-directions-for-the-eu2019s-digital-strategic-autonomy, last accessed September 2021.

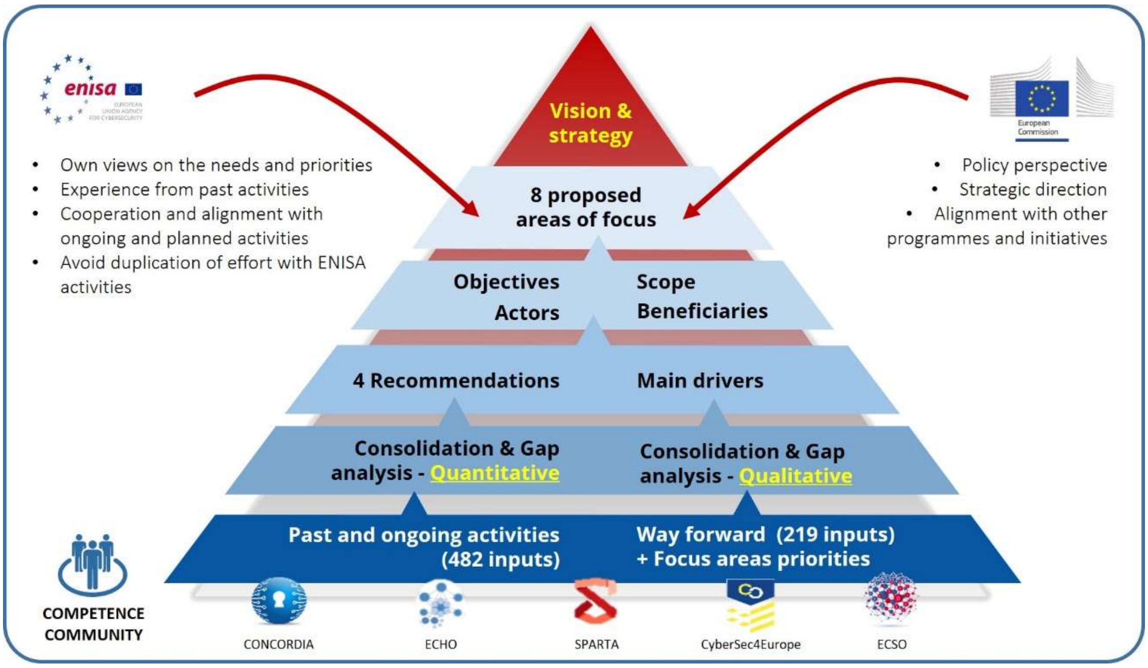
Finally, the European Commission has also contributed to these proposals with comments and recommendations based on its own views and ideas.

ENISA adopted the following structure to present the details, scope and components for each proposal:

- The main driver and objectives;
- Reference to the ECCC Regulation[14];
- Horizon Europe or Digital Europe impact ;
- Entities inputs;
- A review produced by ENISA;
- A baseline with references to past and ongoing work performed by the Entities, other EU funded projects, ENISA and other EUIBAs;
- Main actors and contributors that should be involved in this proposal;
- Who benefits from this proposal;
- And, legal frameworks and other areas to be taken into consideration for this proposal.

To prepare these proposals, the EC and ENISA adopted a bottom-up approach as depicted in figure 2.

Figure 2 - Process adopted


enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
• Own views on the needs and priorities
• Experience from past activities
• Cooperation and alignment with ongoing and planned activities
• Avoid duplication of effort with ENISA activities
European Commission
• Policy perspective
• Strategic direction
• Alignment with other programmes and initiatives
Vision & strategy
8 proposed areas of focus
Objectives
Actors
Scope
Beneficiaries
4 Recommendations
Main drivers
Consolidation & Gap analysis - Quantitative
Consolidation & Gap analysis - Qualitative
Past and ongoing activities (482 inputs)
Way forward (219 inputs) + Focus areas priorities
COMPETENCE COMMUNITY
CONCORDIA
ECHO
SPARTA
CyberSec4Europe
ECSO

[14] https://eur-lex.europa.eu/procedure/EN/2018_328, last accessed October 2021.

1.3 THE PROPOSALS

The European Cybersecurity Competence Centre in its mandate to pool investment into research and innovation in collaboration with the National Coordination Centres, the advice from ENISA and other stakeholders, will create unique conditions for the Cybersecurity Competence Community to generate knowledge, strengthen the Union cyber defences and develop the 'next generation of cybersecurity solutions'.

Chapter 2 of this document presents the results from the analysis conducted to the inputs provided by the Entities, the recommendations produced from a gap analysis and ENISA own views on research and innovation needs and priorities in the field of cybersecurity. As a result from this work, ENISA produced eight draft proposals with the potential to contribute to fulfil this vision in different areas. These proposals are still in a draft state since the process to define a vision for a future strategic agenda for the ECCC will continue in order to achieve a wider consensus from all the stakeholders.

The areas focus identified in this document include, enhancing cybersecurity preparedness; improving the resilience of the EU critical infrastructure and the digital supply chain; develop cyber competencies; stimulation of EU cybersecurity technology production; European cybersecurity cooperation structures, approaches and actors and; human and societal perspective in cyber. Additionally, there is an association between some of these proposals with the impact expected from Horizon Europe (HE) [15] Strategic Plan and Digital Europe Programme[16] (DEP), further explained in this chapter.

The first two proposed areas of focus identify the need for common and unified platforms to support the exchange of knowledge and information. This information is critical for cybersecurity professionals to defend their systems but also for researchers, academia and businesses to support the development of new solutions. The proposals 3 and 4 aim to support the development of cybersecurity competencies at the union level as the main driver for mobilizing the academic and research community into the domain. The proposals 5 and 6 to create mechanisms, tools and platforms to support the daily work of researchers, professionals, entrepreneurs, SMEs, start-ups and other actors on their path to knowledge creation and innovation. In order to develop the 'next cybersecurity solution', it is important that conditions are met to complete the entire development cycle so that products and services are developed, produced and

[15] https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en last accessed July 2021.
[16] https://www.digitaleurope.org/ last accessed July 2021.

later reach the market. The last two proposals related to the functioning of the Competence Centre: proposal 7 highlights the importance of having a network and a platform to support the mobilisation of the Competence Community in the work of the Centre while proposal 8 considers the inclusion of a human and social dimension in EU funded projects and activities. Figure 3 depicts the vision and figure 4 the overall concept with the proposals. In Table 1 below, the proposed areas are grouped according to the span to which the objectives can be achieved (short, medium and long term).

Figure 3 - The vision

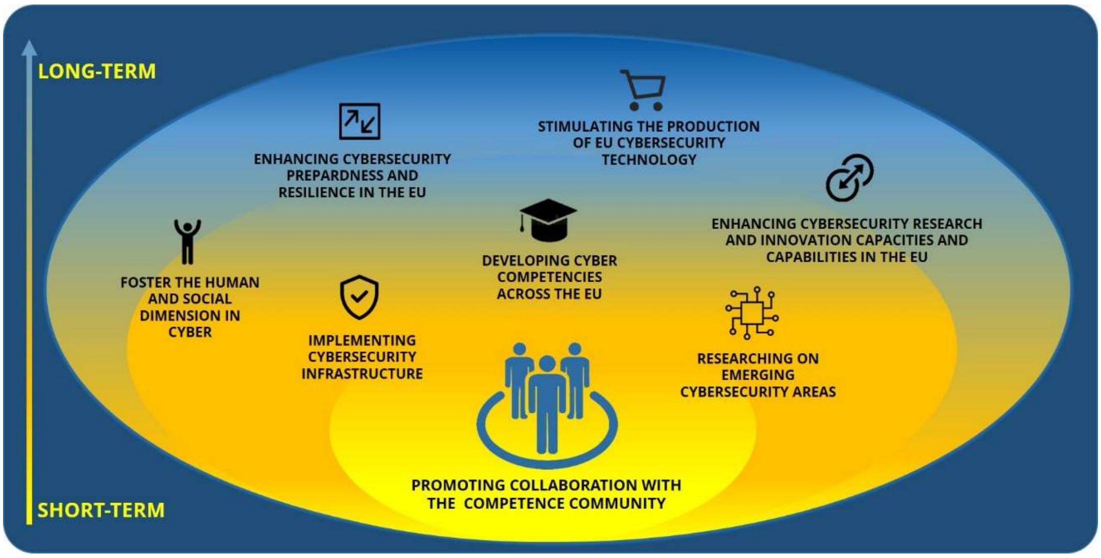

LONG-TERM
STIMULATING THE PRODUCTION OF EU CYBERSECURITY TECHNOLOGY
ENHANCING CYBERSECURITY PREPARDNESS AND RESILIENCE IN THE EU
ENHANCING CYBERSECURITY RESEARCH AND INNOVATION CAPACITIES AND CAPABILITIES IN THE EU
DEVELOPING CYBER COMPETENCIES ACROSS THE EU
FOSTER THE HUMAN AND SOCIAL DIMENSION IN CYBER
IMPLEMENTING CYBERSECURITY INFRASTRUCTURE
RESEARCHING ON EMERGING CYBERSECURITY AREAS
PROMOTING COLLABORATION WITH THE COMPETENCE COMMUNITY
SHORT-TERM

Figure 4 - Overall concept with the proposed areas of focus

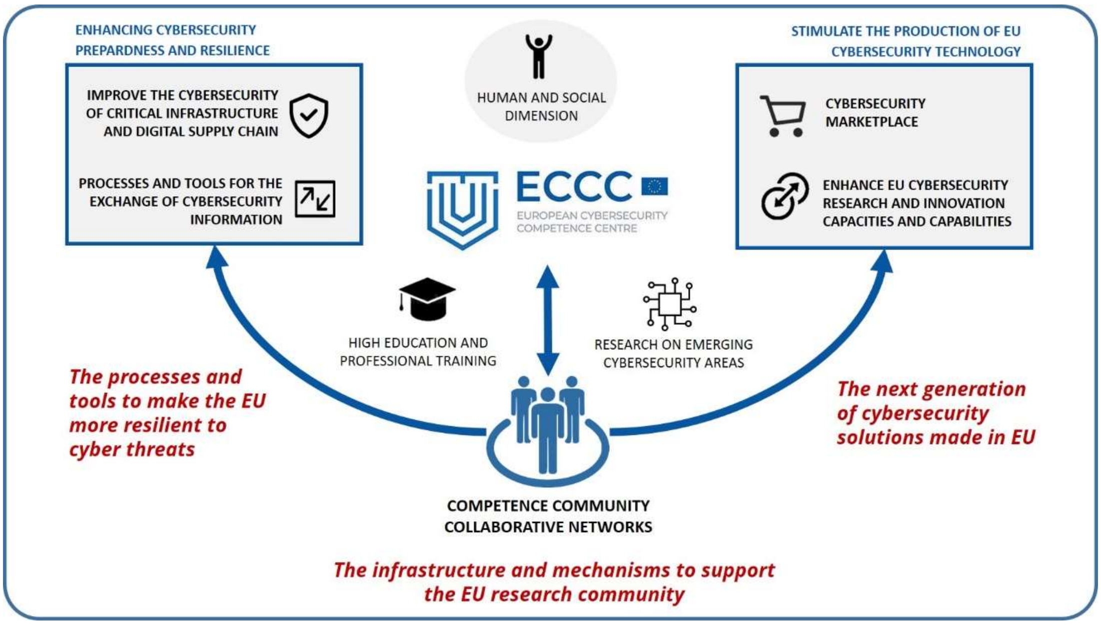

ENHANCING CYBERSECURITY PREPARDNESS AND RESILIENCE
IMPROVE THE CYBERSECURITY OF CRITICAL INFRASTRUCTURE AND DIGITAL SUPPLY CHAIN
PROCESSES AND TOOLS FOR THE EXCHANGE OF CYBERSECURITY INFORMATION
HUMAN AND SOCIAL DIMENSION
ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE
STIMULATE THE PRODUCTION OF EU CYBERSECURITY TECHNOLOGY
CYBERSECURITY MARKETPLACE
ENHANCE EU CYBERSECURITY RESEARCH AND INNOVATION CAPACITIES AND CAPABILITIES
HIGH EDUCATION AND PROFESSIONAL TRAINING
RESEARCH ON EMERGING CYBERSECURITY AREAS
The processes and tools to make the EU more resilient to cyber threats
The next generation of cybersecurity solutions made in EU
COMPETENCE COMMUNITY COLLABORATIVE NETWORKS
The infrastructure and mechanisms to support the EU research community

Table 1 - Summary of the proposals separate by periods of implementation

SHORT-TERM PROPOSALS

#	PROPOSAL	MAIN DRIVERS	ACTORS
2.7	Competence community collaborative networks	EUROPEAN CYBERSECURITY COOPERATION STRUCTURES, APPROACHES AND ACTORS	ECCC, ENISA, Competence Community
2.8	Foster the human a social dimension in cybersecurity	HUMAN AND SOCIETAL PERSPECTIVE IN CYBER	ECCC, ENISA, NCCs, Competence Community

MEDIUM-TERM PROPOSALS

#	PROPOSAL	MAIN DRIVERS	ACTORS
2.2	Improve cybersecurity of critical infrastructure and digital supply chain	RESILIENCE OF THE EU CRITICAL INFRASTRUCTURE AND THE DIGITAL SUPPLY CHAIN.	ECCC, ENISA, NCCs, Competence Community, Industry, OES, DSP
2.4	Common tools and platforms for higher education and professional training	DEVELOP CYBER COMPETENCIES	ECCC, ENISA, NCCs, Competence Community, Universities, Training Institutes, schools
2.5	Research on emerging cybersecurity areas	DEVELOP CYBER COMPETENCIES	ECCC, ENISA, NCCs, Competence Community, EU bodies and agencies such as JRC, ERC, EREA, EIT, among others. EuroQCI, EU research community and academia

LONG-TERM PROPOSALS

#	PROPOSAL	MAIN DRIVERS	ACTORS
2.1	Processes and tools for the exchange of cybersecurity information	ENHANCING CYBERSECURITY PREPAREDNESS AND RESILIENCE.	ECCC, ENISA, NCCs, Competence Community, CTI vendors, CERTs, ISACs, CyCLONe
2.6	Enhance EU cybersecurity research and innovation capacities and capabilities	STIMULATE THE PRODUCTION OF EU CYBERSECURITY TECHNOLOGY	ECCC, NCCs, Competence Community, EU bodies and agencies such as JRC, ERC, EREA, EIT, among others, EU research community and academia

2.7	EU cybersecurity marketplace	STIMULATE THE PRODUCTION OF EU CYBERSECURITY TECHNOLOGY	ECCC, NCCs, Competence Community

Cybersecurity is one of the components of HE program. The main objective is to have an "Increased cybersecurity and a more secure online environment by developing and using effectively EU and Member States' capabilities in digital technologies supporting protection of data and networks aspiring to technological sovereignty in this field, while respecting privacy and other fundamental rights; this should contribute to secure services, processes and products, as well as to robust digital infrastructures capable to resist and counter cyber-attacks and hybrid threats."[17]

According to the HE Strategic Plan, the proposals should contribute to the achievement of one or more of the following impacts:

- Strengthened EU cybersecurity capacities and European Union sovereignty in digital technologies.
- More resilient digital infrastructures, systems and processes.
- Increased software, hardware and supply chain security.
- Secured disruptive technologies.
- Smart and quantifiable security assurance and certification shared across the EU.
- Reinforced awareness and a common cybersecurity culture.

The impacts listed above are reflected in the proposals presented in this document. The strength of these proposals lies in the way they intersect at various points and complement with others from HE projects. For example, cluster #4, which includes digital, industry and space, and DEP complements the proposal to define 'strategies to address cybersecurity challenges from emerging technologies' (#5). In addition, these proposals also build on past and ongoing activities of HE, DEP and CEF[18] funded projects (including the four pilot projects), ECSO and the work of ENISA. Finally, an alignment with the objectives of the Cybersecurity Competence Centre and the National Coordination Centres

[17] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2021-2022/wp-6-civil-security-for-society_horizon-2021-2022_en.pdf last accessed July 2021.
[18] Connected Europe Facility. https://ec.europa.eu/inea/en/connecting-europe-facility last accessed July 2021.

network (Regulation (EU) 2021/887)[19]. The Cybersecurity topics selected for the 2021 Horizon Europe Program are as follows:

- Dynamic business continuity and recovery methodologies based on models and prediction for multi-level Cybersecurity.
- Improved security in open-source and open specification hardware for connected devices.
- AI for cybersecurity reinforcement.
- Scalable privacy-preserving technologies for cross-border federated computation in Europe involving personal data.

[19] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32021R0887 last accessed July 2021.

2. PROPOSED AREAS OF FOCUS FOR FUTURE PROJECTS AND ACTIVITIES

2.1 PROCESSES AND TOOLS FOR THE EXCHANGE OF CYBERSECURITY INFORMATION

Objectives:

- **Enhance cybersecurity preparedness across Europe (main driver).**
- Promote the adoption of common tools and processes for the exchange of contextualized and actionable cybersecurity information[20] across the EU.

HE Impact:

- More resilient digital infrastructures, systems and processes.

ECCC Regulation:

- Article 5 (2)(b)(i)(4) and the strategic tasks of the Centre shall consist of the deployment of cybersecurity products, services and processes.

Overview of the inputs from the Entities

The inputs[21] from #1 to #7 highlight the need to establish common systems and tools for the exchange of cybersecurity information across the EU and also addressing the requirements from sectors and themes. The entities also noted the need to reduce fragmentation and incentivise the use common taxonomies and methodologies for the classification of information.

ENISA views of this proposal

Information exchange is critical to mitigate the risks from the current cyber threat landscape affecting many organisations in the EU. Effective risk analysis, vulnerability disclosure, incident reporting and threat intelligence sharing are important mechanisms for improving cybersecurity preparedness capabilities at national, sectoral and community level. The value of facilitating access to this information lies in the ability to correlate data from multiple sources and enrich the analysis of those at the forefront defending systems, networks, and data from cyber threats. These mechanisms should become widely available to Information Sharing and Analysis Centres (ISACs), National Security Operation Centres (SOCs), Computer Emergency Response Teams (CERTs), and others relevant beneficiaries.

[20] Cybersecurity information includes: threat information, information about malicious behaviour; incident data and vulnerability information.
[21] List of inputs provided by the Entities in Annex 1

ENISA highlights the fact that many processes and tools (including platforms) already exist in Europe from public and private sector organisations, providing contextual and actionable cybersecurity information. This proposal could overlap with ongoing initiatives and activities at the EU level in this domain. However, **the ECCC should organise a call for proposals on the research and development of processes and tools to support an agile and more efficient processing and exchange of contextualised and actionable cybersecurity information, making it widely available to different industries and sectors and preferably for SMEs**.

The ECCC to organise a call for proposals taking into consideration six distinct dimensions as follows:

1. The Centre should provide support to projects dedicated to the research and development of new processes and tools to reduce fragmentation and optimise the collection, processing (analysis) and exchange of contextualised and actionable threat intelligence, incident reports, behavioural analytics and vulnerability information tailored to specific technologies, sectors and domains. This work should also include research and development of solutions to establish pan-European coordination between interrelated sectors focusing on the synchronized exchange of cyber threat intelligence between priority industries including space, defence and other critical sectors.
2. The wealth of information acquired in SOCs remains enormous, posing a significant challenge to cyber defenders. The Centre should provide support to research projects focussed on the development of algorithms enabling the automation of data analytics and correlation of cybersecurity information from multiple sources, context, formats and use-cases. Research projects that should also include the use of big-data analytics, artificial intelligence and machine learning to deal with a high volume and high variety of cybersecurity data available. The use of innovative tools to automate some the most labour-intensive tasks in cybersecurity will increase efficiency and optimise the decision making processes in critical and time-sensitive operations.
3. The Centre should provide support to projects aiming at the research and development of application of programming interfaces (APIs), web services, database federation schemes and using machine-readable formats to promote the exchange of cybersecurity information across trusted platforms, technologies, networks, etc. The results from the research on these APIs should become widely available to all existing and new platforms as a standard for the exchange of cybersecurity information.
4. The Centre should provide support to projects that research the complexity and diversity of current IT systems, SIEM and SOAR platforms to find innovative ways on how to expand and provide operators with a complete view of the situation. Research should also include the development of methods to raise awareness and improve training for operators to

keep up with threats. New data streams, e.g. from ISACs, will also help operators to become familiar with the view of the application sector.

5. The Centre should provide support to projects dedicated to the research of innovative deception mechanism such as 'honeypot' could provide effective triggering alerts related to malicious activity. This area could include exploring adversarial machine learning techniques to learn more about attackers leveraging AI tools to deploy advanced attack schemes.
6. The Centre should support future research looking beyond technology and where there is a need to establish and promote trusted forums for sharing cyber threat information and where incident data can be shared in detail with a limited community. ISACs are important players in developing these community forums and improving European cyber security preparedness.

Baseline:

- **ENISA** has for many years contributed with guidelines and good practices in the collection, analysis and exchange of cybersecurity information. The work of ENISA in the preparation of threat[22] and incident classification[23] taxonomies is a main reference for this proposal.
- The European Commission **Join Research Centre (JRC)**, in collaboration with the four Pilot Projects and ECSO, made a proposal for a common European Cybersecurity Taxonomy[24]. The proposed taxonomy aligns cybersecurity definitions and terminologies to enable the categorisation of existing institutions and expertise across Europe. This categorisation is crucial to facilitate the potential collaboration among these institutions and consequently to foster the establishment of the Competence Centre and Network.
- The **CyCLONe** is a cooperation network for Member States with the aim to contribute to the implementation of the European Commission's Blueprint[25] for rapid emergency response in case of a large-scale cross-border cyber incident or crisis and complements the existing cybersecurity structures at EU level by linking the cooperation at technical (e.g. Computer Security Incident Response Team – CSIRTs) and political levels (e.g. Integrated Political Crisis Response – IPCR).
- A threat intelligence platform from **CONCORDIA** and the correlation engines complete the system to provide gathering of threat information and their correlation to incidents and warnings.
- **SPARTA** developed a cybersecurity threat intelligence common data model.

[22] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view, last accessed October 2021.
[23] https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy, last accessed October 2021.
[24] https://publications.jrc.ec.europa.eu/repository/handle/JRC118089, last accessed October 2021.
[25] https://eur-lex.europa.eu/eli/reco/2017/1584/oj, last accessed September 2021.

- **ECHO** Multi-Sector Assessment Framework (E-MAF) with the aim to trace and compute the risk in multisector scenarios.
- The **'No More Ransom'**[26] project is an initiative by the National High Tech Crime Unit of the Netherlands' police, Europol's European Cybercrime Centre, Kaspersky and McAfee with the goal to help victims of ransomware retrieve their encrypted data without having to pay the criminals.
- The **CYBER-TRUST**[27] project aimed to develop an innovative cyber-threat intelligence gathering, detection, and mitigation platform to tackle the grand challenges towards securing the ecosystem of IoT devices.
- Europe has invested a significant amount of effort in cyber threat intelligence, for example the **Malware Information Sharing Platform (MISP)**[28] and the **OpenCTI**[29] open-source software. These efforts should be sustained to ensure that Europe is able to influence standards currently under development at the Internet Engineering Task Force (IETF) or the European Telecommunications Standards Institute (ETSI).

Actors and contributors:

- The **ECCC** is responsible for attracting the most excellent researchers and innovative enterprises to participate in the programme and present proposals for financial support. The Centre is responsible for organising a call for proposals addressing the areas outlined in the Work Programme and aligned with the Strategic Agenda.
- **ENISA** to contribute to the definition of requirements based on the knowledge and expertise from preparing an interoperable risk management framework, supporting the establishment, development and cooperation of European information-sharing schemes based on ISACs, public–private partnerships and other existing mechanisms; supporting the functioning and operations of the CSIRTs Network (including through MeliCERTes and CyCLONe group and cyber crisis management in the EU); generating and consolidating information (including for the general public) on cyber situational awareness, technical situational reports, incident reports and information on threats and support the consolidation and exchange of information at strategic, tactical and technical levels; and monitoring and documenting the dependencies and vulnerabilities of IICT products and services[30]. ENISA also coordinates with key EU stakeholders such as CERTs, ISACs, JCU, JRC, EUROPOL, EDA, NCSAs and others, to define the needs and use cases, classification criteria for the collection, analysis and sharing of cybersecurity information.

[26] https://www.nomoreransom.org, last accessed October 2021.
[27] https://cordis.europa.eu/project/id/786698, last accessed October 2021.
[28] https://www.misp-project.org/, last accessed September 2021.
[29] https://www.opencti.io/en/, last accessed September 2021.
[30] ENISA Single Programming Document 2021-2023 outputs 3.4, 3.6, 5.1 and 7.4

- The **Competence Community** to present proposals and deliver the platforms and interfaces for the collection, analysis and sharing of cybersecurity information.
- **EU Institutions, Bodies and Agencies (EUIBAs)** involved in the analysis and processing of threat assessments and intelligence e.g. EEAS, EUROPOL, CERT-EU and European Defence Agency (EDA).

Legal frameworks and other areas to take into consideration:

- The Directive on Security of Networks and Information Systems (NISD) require that critical infrastructure operators report cybersecurity incidents to the authorities and inform their peers through Information Sharing and Analysis Centres (ISACs).

Beneficiaries:

- At a national level CERT Community and National Cybersecurity Authorities.
- At sectoral level ISACs and CERTs.
- ENISA Operational Cooperation with a link to the future Joint Cyber Unit (JCU)[31].
- Operators of essential services and digital services providers.
- Other relevant communities.
- SMEs.

2.2 IMPROVE CYBERSECURITY OF CRITICAL INFRASTRUCTURE AND DIGITAL SUPPLY CHAIN

Objectives:

- **Improve the resilience of the EU critical infrastructure and the digital supply chain to cyber threats (main driver).**

HE Impact:

- More resilient digital infrastructures, systems and processes.
- Increased software, hardware and supply chain security.

ECCC Regulation:

- Article 5 (2)(b)(i)(6): support for the adoption and integration of state-of-the-art cybersecurity products, services and processes by public authorities at their request, by demand-side industries and by other users.

Overview of the inputs from the Entities

Concerning cybersecurity of EU critical infrastructure, the Entities provided inputs from #14 to #18 highlighting the need to develop self-assessment tools, methods and standards in support of the NIS Directive implementation and to work on the harmonisation of standards for incident reporting across the EU.

[31] https://ec.europa.eu/commission/presscorner/detail/en/IP_21_3088, last accessed June 2021.

Concerning cybersecurity of the digital supply chain, the Entities provided inputs #4, #5, #10, #13 and #15 highlighting the need to establish common risk assessment methods and tools to improve the cybersecurity in the digital supply chain. The Entities also identified the need to prepare a future vendor certification mechanism and to define incident reporting requirements for digital supply-chain security.

ENISA views of this proposal

2.2.1 Cybersecurity of EU critical infrastructure

Critical infrastructures systems like those driving water treatment, power generation, power production, telecommunications and others have always been an attractive target for malicious actors[32]. One of the main reasons is because their services are essential for the functioning of society and the economy.

Whether it is a physical infrastructure (e.g., a bridge, a road), a complex interconnected infrastructure (e.g., a physical/digital supply chain, operational technology, industrial control systems, distributed controls systems), or even the Internet itself, critical infrastructures together with their control systems can cause or enable major (sometimes irreparable) damage, if they are manipulated and/or cease to operate. As such, it is essential to devise novel security and privacy solutions that not only protect intertwined information technology assets in federated ecosystems, but also facilitate the secure and private collaboration between all physical and digital actors.

The ECCC should organise a call for proposals to support the research and development of innovative applications to improve the cyber protection of critical infrastructure.

The proposed research should focus on addressing the challenges introduced by:

- inexistent specific risk-models for mission critical systems and digital supply chains;
- legacy technologies still in use by many operators of essential services without adequate security processes and maintenance that cannot be protected;
- the lack of security orchestration and response to deal with cascading failure;
- the lack of preparation and dissemination of cyber situational awareness;
- missing incident reporting, early warning systems and other mechanisms specifically design for the notification of operators of essential services and digital service providers and;
- the lack of cybersecurity visibility over the Operational Technology (OT) environment;

Over the past few decades, the cybersecurity industry has put considerable effort into developing numerous intrusion detection and network monitoring tools. However, the difficulty of deploying them has led to the emergence of SOCs as managed security services to facilitate deployment and

[32] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents, last accessed September 2021.

operation for organisations that do not have the skills and resources to deploy such services. Europe must preserve and enhance its ability to develop and deploy EU-developed detection sensors in its most critical infrastructures. It must also maintain its ability to develop and deploy SIEM and SOAR platforms, including open source alternatives where commercial components cannot be sourced in Europe.[33]

2.2.2 Cybersecurity in the digital supply chain

The supply chain has become a more attractive target for malicious actors because it can have a larger-scale and cross-border impact[34]. This situation has led to an increase in the number of successful attacks over the last 2 years. To ensure the growth of the Digital Single Market and the digital economy, it is important that EU citizens, businesses and organisations trust the technology and the entire value-chain supporting it.

To improve security in the digital supply chain, it is important to take a risk-based approach. One of the benefits of this approach is that it guides the decision-making process of accepting or rejecting an entity from participating in the supply chain. Most importantly, it helps an efficient mitigation of cybersecurity threats that third parties can pose to the entire supplier ecosystem.

The use of risk assessment methodologies and tools is important to assess the maturity and security posture of a participant in a supply chain. They can identify and rank third-party relationships by risk criticality and help define risk criteria for different types of suppliers and services. The results of a risk assessment helps defining risk mitigation measures required to join the supply chain.

The ECCC should organise a call for proposals to support the research and development of security assessment and evaluation methodologies and tools or the extension of an existing methodology, to cover the specificities of digital supply chains.

This proposals considers the development of collaborative tools and services specifically designed to manage risk across the ecosystem. ENISA has developed recommendations to improve supply chain security. These recommendations are valid for defining the requirements of the methods and tools considered in this proposal. The following list summarises recommendations from the ENISA study and inputs from the Entities, to be considered in the requirements for future call for proposals organised by the ECCC. The Centre should support projects aiming at:

- the research and development of methods and tools to support the management of the relationship between suppliers and customers of digital products, processes and services;

[33] https://www.enisa.europa.eu/publications/cybersecurity-research-directions-for-the-eu2019s-digital-strategic-autonomy, last accessed September 2021.
[34] https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks, accessed September 2021.

- the research and development methods and tool to help suppliers ensuring the secure development of digital products and services that are consistent with commonly accepted security practices, standards and certifications;
- the research and development methods and tools to implement good practices for vulnerability management;
- the research and development of vendor certification mechanisms and standard incident reporting requirements for digital supply-chain security;
- the research of secure software development platforms to ensure that the systems meet specific security requirements;
- the research and development of security third-party libraries and services that are independent and beyond the control of software developers.

Baseline:

- **ENISA** produced a study on supply chain integrity: an overview of the ICT supply chain risks and challenges, and vision for the way forward[35] and is currently working on 'coordinated and interoperable risk management frameworks'.
- **ECHO** Early Warning System designed as a main early warning/incident management/ information sharing system works at multiple layers of abstraction from incident management to C-level overview, from national to sector-specific, up to transnational.
- The **CAPE program** developed by **SPARTA** includes tools to validate software, including aspects relevant for the software supply chain (e.g. vulnerabilities in libraries and build processes).
- **CyberSec4Europe** developed cross-stakeholder risk analysis, mitigation methods and tools (cyberwatching.eu). It also developed a decentralized approach using distributed ledger technology to manage access to supply chain data, log data securely and address non-repudiation and accountability.
- **TOP-IT[36]** focuses on the strategic, tactical and operational protection of critical water infrastructures against physical and cyber threats.
- **SOCCRATES[37]** aims to develop and implement a new security platform for Security Operation Centres (SOCs) and Computer Security Incident Response Teams (CSIRTs) of individual organisations and offered by Managed Security Service Providers (MSSP).
- **CyberSANE**[38] enhances the security and resilience of Critical Information Infrastructures (CIIs) by providing a dynamic collaborative, warning and response system supporting and

[35] https://www.enisa.europa.eu/publications/sci-2015, last accessed September 2021.
[36] https://stop-it-project.eu/, last accessed September 2021.
[37] https://www.soccrates.eu, last accessed October 2021.
[38] https://www.cybersane-project.eu, last accessed October 2021.

guiding security officers and operators to recognise, identify, dynamically analyse, forecast, treat and respond to advanced persistent threats (APTs).

- **PANACEA**[39] delivers a dynamic risk management platform for the healthcare sector to respond more swiftly to the risks of a complex and multi-faceted threat landscape while fostering positive behavioural changes.
- **Cyber-MAR**[40] aims to develop an innovative cybersecurity simulation environment for accommodating the peculiarities of the maritime sector while, being easily applicable in other transport subsectors, with the view to fully unlock the value of the use of cyber range in the maritime logistics value chain.

Main actors and contributors:

- The **ECCC** is responsible for attracting the most excellent researchers and innovative enterprises to participate in the programme and present proposals for financial support. The Centre is responsible for organising a call for proposals addressing the areas outlined in the Work programme and aligned with the Strategic Agenda. Article 5 (2)(b)(i)(6) of the ECCC regulation states that the Centre is supposed to support for the adoption and integration of state-of-the-art cybersecurity products, services and processes by public authorities at their request, by demand-side industries and by other users.
- **ENISA** to contribute to the definition of requirements based on the knowledge and experience from the guidelines and tools promoting 'security by design' and 'security by default' measures for ICT products, services and processes; the development and maintenance of an EU cybersecurity certification framework; the support to Member States and the European Commission in the implementation of the 5G security toolbox and; from individual actions on coordinated and interoperable risk management frameworks[41]. ENISA and the **CyberShield (SOCs Network)** to maintain continuous situational awareness and provide an EU perspective to the requirements**.**
- The **Competence Community** to present proposals for the design and development of the methods and tools.

Legal frameworks and other areas to take into consideration:

- The Directive on Security of Networks and Information Systems (NISD and NISD 2.0);
- The proposal for a regulation on Digital Operational Resilience for the Financial Sector (DORA)[42];

[39] https://www.panacearesearch.eu/, last accessed October 2021.

[40] https://www.cyber-mar.eu/, last accessed October 2021.

[41] ENISA Single Programming Document 2021-2023 outputs 3.4, 4.1 and 5.1

[42] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&from=EN last accessed September 2021.

- Involvement of Information Sharing and Analysis Centers (ISACs) in the definition of requirements.
- The Connecting Europe Facility (CEF) programme[43] contributes to the deployment of and access to safe and secure very high capacity digital networks and 5G systems, support an increased security, resilience and capacity of the digital backbone networks in the EU.

Beneficiaries:

- Operators of essential services and digital services providers.
- Technology industry;

2.3 COMMON TOOLS AND PLATFORM FOR HIGHER EDUCATION AND PROFESSIONAL TRAINING

Objectives:

- **Develop cyber competencies (main driver).**
- Introduce educational curricula aligned with the needs of the industry, businesses and organisations.

DEP Impact:

- By 2025, Europe should strive to invert the increasing gap of cybersecurity professionals that it requires.

ECCC Regulation:

- Article 5 (2)(b)(i)(3): the reinforcement of cybersecurity and technology skills and competence in industry, technology and research and at all relevant educational levels, supporting gender balance.

Overview of the inputs from the Entities

The inputs from #22 to #26 highlight the need to implement a one-stop platform for cybersecurity in higher education, organise specialised programs in cybersecurity professional training at a local, sectoral and regional level and organise an annual European forum on the rollout of the European Cybersecurity Skills Framework (ECSF).

ENISA views of this proposal

This proposal stems from an ENISA recommendation: ***Consolidate a vision for the development of cybersecurity competencies across EU communities***[44], based on a review conducted on past and present activities performed by the four Pilot Projects and ECSO.

[43] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2021.249.01.0038.01.ENG&toc=OJ%3AL%3A2021%3A249%3ATOC, last accessed October 2021.

[44] ENISA recommendations listed in Annex 1 of this document.

The EU's investment in cybersecurity capacity building over the past decade demonstrates its commitment to ensuring that its citizens, businesses and organisations are ready to deal with cyber threats and to further improving the Union's cybersecurity preparedness. However, there is still a long way to go to close the gap in the EU's cybersecurity capabilities. Given the increasing complexity of the threat landscape and the rising number of incidents[45], it is now more important than ever to leverage from the results and develop the programmes and solutions to further increase the number of students and trained professionals in cybersecurity as well as prioritise the development of skills and competencies mostly-in-need in the workforce.

The ECCC should organise a call for proposals focused on the development and implementation of tools/platforms to support and host higher education, professional training resources and initiatives with the aim of, building capacity and developing skills in the field of cybersecurity. In this proposal, there are six distinct dimensions. The Centre should provide support to projects aiming at:

1) The rollout of the European Cybersecurity Skills Framework (ECSF). The aim of this framework is to create a common understanding of the roles, competencies, skills and knowledge used by and for individuals, employers and training providers across the EU Member States in order to address the cybersecurity skills shortage and gap. ECSF is designed to be a multi-stakeholder tool with the goal to promote harmonization in the ecosystem of cybersecurity education, training, and workforce development. The finalization of this framework will allow to identify skills and competence mostly in need in Europe and create learning paths in order to address the cybersecurity skills gap. It will also promote initiatives to link demand and supply of cybersecurity professionals in Europe. The Centre should provide support to projects aiming at the implementation of the ECSF with dedicated competence/job portals as well as tools for matchmaking, leveraging cyber ranges and exercise environments, and skills verification approaches.
2) The development of a framework for higher education in the field of cybersecurity. The Competence Centre to support projects aiming to increase the number of graduates in cybersecurity through the development of cybersecurity courses and professional development training activities in higher education programmes and align it with the competencies and skills required by the job market. The goal of this proposal is to leverage the experience from the existing and ready-to-use CYBERHEAD portal[46], developed by ENISA in cooperation with two of the Pilots Projects. A one-stop shop for cybersecurity upskill and reskill required in the EU in order to incentivize individuals to study cybersecurity and provide academic learning path to the cybersecurity professional roles. The one-stop shop portal will be able to attract a variety of individuals interested to benefit of the career prospects in cybersecurity, through the strong connection to ECSF job portal, and help educational institutions to build cybersecurity curricula.

[45] https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020, last accessed September 2021.
[46] https://www.enisa.europa.eu/cyberhead last accessed July 2021

3) The research on the use of gamification and artificial intelligence to model cybersecurity problems used in trainings and exercises. From a technological perspective, the Competence Centre should create incentives for researchers to look into autonomous training solutions using reinforcement learning to simulate adversarial scenarios in corporate environments. Similarly, experiences with gamification techniques should be created to train adversarial algorithms that challenge cyber defence capabilities.

4) The development and implementation of open source platforms for cybersecurity training, including cyber ranges, exercises arenas. The Centre should also support projects aimed at increasing the number of and facilitating the access to cybersecurity training infrastructures such as learning resources, cyber ranges and exercises arenas. Also, establishing full-fledged open-source cyber training infrastructures for higher education is an important contribution to the learning process due to it is practical and experimental nature. These training infrastructures are tools that can support the creation of actionable and realistic training scenarios based on real-life information. The proposal also foresees the creation of a 'European Cybersecurity Training Community' responsible for maintaining the technical infrastructures to support training and exercises. An infrastructure characterised by its interoperability and connectivity between EU cybersecurity training facilities maintained by different members of the Competence Community. Other important features such as sector specialisation, cross-border and cross-sector coverage should also be taken into account.

5) The work on the standardisation of professional training in cybersecurity**.** Industry and service providers to standardise the professional training curriculum and contribute with proposals for a future European cybersecurity certification schemes for professional training. The proposed platform could serve as an enabler and pathfinder for mapping programmes, courses and training offerings, starting at the university level.

6) The definition of a professional career in cybersecurity**.** Provide information about possible career options in cybersecurity for high school graduates and new comers into the profession, by highlighting the different role profiles within an organisation.

Baseline:

- **ENISA** is very active running exercises, developing training programmes and supporting the Competence Community to define the ECSF.
- **ECSO**'s European Human Resources Network for Cyber (EHR4CYBER) Task Force[47] creates awareness among decision makers (private companies, regional / local administrations, national / EU administrations) about the need to develop education and training measures, which will address the demand in the cybersecurity field.

[47] https://exed.solvay.edu/images//2018_EHR4CYBER-WG5_white-paper_information-and-cyber-security-professional-certification_final_v0.1-1-1.pdf, last accessed July 2021.

- **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. The app named 'Curricula Designer'[48] 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.
- **ECSO** delivered a position paper on Gaps in Education & Professional Training and is currently working on EHR4CYBER[49]: a link to HR / survey to understand recruitment practices; and WOMEN4CYBER[50], a platform to facilitate access to training and offers of in-kind trainings.
- **CONCORDIA** introduced an interesting concept with an Open format for sharing cybersecurity training. This will improve cybersecurity training development and lower training costs for organizations.
- Several ongoing activities aim to refine technologies and develop standard languages to describe cyber range scenarios and map capacity-building objectives. For example, **KYPO CRP**[51] from **CONCORDIA** was designated as a 'key innovation' by the EC Innovation Radar[52]. Almost all Entities are very active on cyber ranges but with different approaches.
- **Cyber Sandbox Creator (CSC)[53]** is a lightweight virtual lab environment for cybersecurity education, testing, and certification. The CSC is being actively developed (plans to release v 2.0.0 this year) and is fully open source (version 1.0.1).
- **EU CyberNet[54]** strengthens the global delivery, coordination and coherence of the European Union's external cyber capacity building projects and to reinforce the Union's own capacity to provide technical assistance to third countries in the field of cybersecurity and cybercrime.

Actors and contributors:

- The **ECCC** is responsible for attracting the most excellent researchers and innovative enterprises to participate in the programme and present proposals for financial support. The Centre is responsible for organising a call for proposals addressing the areas outlined in the Work programme and aligned with the Strategic Agenda. Article 5 (2)(b)(i)(3) of the ECCC regulation states the reinforcement of cybersecurity and technology skills and competence in industry, technology and research and at all relevant educational levels, supporting gender balance.

[48] https://sparta.eu/curricula-designer/, last accessed June 2021.
[49] https://ecs-org.eu/working-groups/wg5-education-training-awareness-cyber-ranges, last accessed June 2021.
[50] https://women4cyber.eu/, last accessed June 2021
[51] https://www.concordia-h2020.eu/news/new-release-of-kypo-crp-brings-support-for-windows-machines/, last accessed June 2021.
[52] https://www.innoradar.eu/, last accessed June 2021.
[53] https://gitlab.ics.muni.cz/muni-kypo-csc/cyber-sandbox-creator accessed July 2021.
[54] https://www.eucybernet.eu/, last accessed October 2021.

- **ENISA** to support the rollout of the ECSF and contribute with guidelines for exercises and the definition of new frameworks. ENISA also reports on cybersecurity skill needs and gaps, and support skills development, maintenance and implementation (including the Digital Education Action Plan and a report on higher education programmes) and organises training and other activities to support and develop the maturity and skills of CSIRTs (including NIS directive sectorial CSIRTs) and other communities[55].
- The **NCCs** and the **Competence Community** to facilitate and present proposals for the design, development and maintenance of the mentioned platform as well as with the rollout of the ECSF.
- European Centre for the Development of Vocational Training (**CEDEFOP**).
- Universities, training institutes and schools.

Beneficiaries:

- EU citizens, students and cybersecurity professionals.

2.4 RESEARCH ON EMERGING CYBERSECURITY AREAS

Objectives:

- **Develop cyber competencies (main driver).**
- Promote research and development of cybersecurity solutions (products, services, and processes) aimed at protecting emerging technologies and other key areas.

HE Impact:

- Secured disruptive technologies.

DEP Impact:

- By 2025, 10% of research and Innovation spending should be targeted at ICT technologies.

ECCC Regulation:

- Article 5 (2)(b)(i)(2): the development of cybersecurity industrial, technological and research capacities, capabilities, and infrastructure.

Overview of the inputs from the Entities

The Entities provided a roadmap consolidating a cybersecurity agenda on research challenges of high-priority for the EU. Moreover, the entities also referenced in inputs from #28 to #31 the need for more research in the security for digital solutions in mobility (people and goods), smart cities, smart governments, space, of AI algorithms (Life-cycle), Biotechnology, NextGen of Internet, machine-to-machine communication (including IoT, ICS, robotics, etc.) for strategic verticals to the EU economy/industry, quantum computing and 6G.

[55] ENISA Single Programming Document 2021-2023 outputs 3.3 and 3.8

ENISA views of this proposal

In this era of transformation, it is critical to invest time and resources to anticipate the challenges and examine the risks that may arise from adopting and adapting to new and emerging technologies. This anticipation is key to the success of the EU Digital Marketplace (DSM) and to protecting EU citizens, businesses and organisations from cyber threats when using cyber space. One of the key issues for the success of the DSM and a safer use of cyber space is to build trust between the various actors when using digital technologies. Without a safe and secure environment, the DSM will not be able to attract companies to do business across EU borders. To contribute to the success of the DSM, it is important to anticipate the challenges and explore the risks posed by emerging and future technologies.

The ECCC should organise a call for proposals focused on exploring the challenges and opportunities in research of emerging and future areas of cybersecurity not only in technological but also in economic, social and political domains.

2.4.1 Secure artificial intelligence (AI)

AI is one of the most transformative forces of our time and a major enabler of the digital economy and the DSM. The importance and extension of its influence is referenced across many other technologies. AI is rapidly changing how businesses and organisations operate, manage data and interact with users in a blend of three advanced technologies: machine learning (ML), natural language processing (NLP) and cognitive computing. With vast advancements in ML, AI is entering a crucial stage in its development path. Researchers in AI are harnessing the explosion of digital data and computational power with innovative algorithms, stimulated in part by the rise of the digital economy. It is becoming critical to define AI-based systems to increase trust in the decision process. Some areas of particular interest for research and innovation include (but not limited to):

- Development of a standardized performance evaluation framework,
- Design of approached monitoring large-scale and possibly interconnected systems,
- Exploration of biomimetic cybersecurity algorithms,
- Incorporation of the security-by-design concept and resilience to adversarial attacks,
- Preservation of privacy and confidentiality of the information flow, and
- Inclusion of context awareness in ML in order to boost resiliency.

2.4.2 AI-based security

Artificial Intelligence (in particular Deep Learning and Machine Learning), together with advances in computing capacity, enable users to process very large amounts of data. As such, AI techniques have been successfully applied to tackle many cybersecurity problems via advanced methods for threat detection, prediction, and response. For example, AI mechanisms have the ability to combat the spread of digital fake assets, which are abused for misinformation and miseducation within our societies. The use of AI as a technology for building system monitoring techniques and anomaly detection should be developed further. At the same time, concerns have been raised over the security and stability of the AI algorithms used in cybersecurity applications. Thus, it is important to ensure that only certified, fair, and security-compliant AI algorithms are used to enhance cybersecurity. This is part of the specific focus area 'Secure AI Systems' described below.

- AI-based security services e.g. predictive security, advanced anomaly and intrusion detection, system health checks.
- Robust AI-based fake detection e.g. audio, video, images and speech.

2.4.3 End-to-end data protection

Data protection is one of the rights in Article 8 of the EU Charter of Fundamental Rights[56] and the introduction of the General Data Protection Regulation[57] (GDPR) has created an obligation to protect personal data in the EU. It has had a global impact on countries and companies, leading to changes in laws and practices also outside Europe.

Recent advances in digital technologies have led to an increasing storing and processing of personal and otherwise sensitive data while connected to the Internet. As a result, (cyber) attackers are constantly finding new ways to 'exfiltrate' sensitive data, leading to a large number of breaches. To make matters worse, some companies do not even know about their data breaches until their data goes public. To reduce the risk and potential impact of data breaches, data must be protected throughout its lifecycle, from collection or creation to storage, processing, and disposal. This includes carefully assessing whether the data is actually needed for its intended purpose and providing stakeholders with tools to make this assessment. In addition, user-centric privacy technologies must be developed to put individuals back in control of their data, along with comprehensive approaches to access management concepts to ensure that only legitimate users are able to access sensitive information. Finally, advanced digital forensics must support the identification of attackers and attack vectors in the event of an intrusion, so that developers and system administrators can further enhance the security of their systems.

- User-Centric Data Governance: self-sovereign data governance.
- Secure End to End Data Life Cycles: secure data acquisition, storage, transfer, processing and deletion.
- Identity & Access Management.
- Digital Forensics.

2.4.4 Secure Biotechnology (Cyberbiosecurity)

[56] European Union, *Charter of Fundamental Rights of the European Union*, C 326/02, Brussels, 26.10.2012, pp. 391–407.
[57] https://gdpr.eu/, last accessed September 2021.

CyberBioSecurity aims to identify and mitigate security risks fostered by the digitization of biology and biotechnology automation. With the current global effort to combat the SARS-CoV-2 pandemic and the use of biotechnology to produce a vaccine, the attention to CyberBioSecurity has increased. Some areas of particular interest for research include (not exhaustive list):

- Envision the various layers of CyberBioSecurity, from cyber-only to those that exploit unknown factors fostered,
- Getting a detailed understanding of CyberBioSecurity vulnerabilities that are clearly different from `cyber-only' threats.
- Targeting the problem of ‘identification' at all levels from molecular to gross.

2.4.5 Secure architectures for the next generation of communications

In this decade, EU researchers and industry will continue to look for new ways to improve and optimize the communications infrastructure to meet the ever-increasing demand for greater connectivity, coverage and availability. It is important to ensure that along with the development of any future generation of communication a comprehensive security research programs follows, to assess and mitigate the risk in a way that promotes trust in the use of the telecommunications infrastructure. The European Union is already paving the way to lead the research and development of the next generation of mobile communications or 6G. This proposal considers the research of cybersecurity requirements for the security of the next generation of mobile communications.

- Secure the next generation of communication systems.
- Responsible internet.

2.4.6 Personal data protection

The digital transformation is encouraging the emergence of new scenarios where a large volume of data is shared and employed to enhance common services. Despite its advantages, this technological evolution is also bringing new security and privacy challenges related to the treatment of such data, especially in case of personal information, where an improper use could violate people’s privacy. As such, different Privacy Enhancing Technologies need to be explored in order to protect and facilitate privacy-respecting sharing personal data, such as secure multi-party computation or fully-homomorphic encryption. Given the rapid digital transformation, continuous research activities are focusing on, e.g., scalability, long-term security, and flexibility of such technologies. However, ensuring data privacy is a task that requires more than just applying a predefined set of techniques or technologies, as it has more requirements, such as legal regulations and individual privacy preferences. Therefore, every system that is handling sensitive data should also collect and record the privacy preferences of the individual to whom the data refers, also known as data subjects.

- Advanced Privacy Protection Requirements, stemming e.g. from social media technologies, precision medicine applications

2.4.7 Secure Quantum technologies

Over the next few decades, demand for quantum computers will be driven by research and development projects and the emergence of various applications, including advanced artificial intelligence algorithms, next-generation encryption, traffic guidance and planning, the study of molecules, protein synthesis, and/or the design of advanced chemicals and materials. The various attempts to develop a quantum computer that is stable and has a low error rate have required heavy investments in infrastructure, software development, and human expertise. It is therefore not surprising that quantum computers are unlikely to reach the level of widespread use of classical computers within the next decade. Nevertheless, some experiments are currently being conducted at extremely low temperatures, in a strong magnetic field, and in a vacuum or sterile environment. Hence, this proposal advocates for cybersecurity associated to quantum computing research, including in the development of quantum computers, quantum communication, quantum key distribution, quantum cryptography, quantum simulators, etc.

- Secure Quantum & Hybrid Computing.
- Secure Quantum Communications.
- Quantum Cryptography.
- Post-Quantum Futures.

2.4.8 Space cybersecurity

Space is becoming increasingly important to many sectors of society and the economy. The growing reliance on telecommunication infrastructures, geo-positioning or the need for geo-mapping and cartographic systems makes these services crucial factor for the operation of many ground-based businesses and organisations. This proposal addresses the exploration of cybersecurity products, processes and services adapted to the technology and requirements of the space environment.

Baseline:

- **ENISA** maintains a foresight capability attempting to describe emerging cybersecurity challenges and opportunities during the next decade. Furthermore, the Agency produces annual reports reviewing cybersecurity challenges from emerging technologies (e.g. autonomous vehicles, artificial intelligence, 5G, quantum computing).
- **CyberSec4Europe** focused on several new technologies such as IoT, AI, privacy preservation, etc. and how they can be integrated within existing cybersecurity enablers.

- The **SAFAIR**[58] program from **SPARTA** conducts a thorough analysis of the threats and risks and detects adversarial attacks on AI.
- The **CiViQ**[59] project developed quantum-enhanced physical layer security services that can be combined with modern cryptographic techniques, to enable unparalleled applications and services.
- The European Quantum Communication Infrastructure **(EuroQCI)**[60]**, 5G-PPP** and 5G Infrastructure Association[61] maintain research projects and working groups in the security of these emerging technologies.
- European Space Security and Education Centre (**ESA ESEC**)[62] is a centre of excellence for space cybersecurity services, home to ESA's Proba mission control centres, the Space Weather Data Centre[63] as well as part of ESA's ground station network.
- **CARAMEL**[64] is a project that aims to introduce an innovative anti-hacking intrusion detection/prevention systems for the European automotive industry by applying advanced Artificial Intelligence (AI) and Machine Learning (ML) techniques.
- **AI4HEALTHSEC**[65] proposes a state of the art solution that improves the detection and analysis of cyber-attacks and threats on HCIIs, and increases the knowledge on the current cyber security and privacy risks.
- The **Human Brain Project**[66] aims to put in place a cutting-edge research infrastructure that will allow scientific and industrial researchers to advance our knowledge in the fields of neuroscience, computing, and brain-related medicine.

Actors and contributors:

- The **ECCC** is responsible for attracting the most excellent researchers and innovative enterprises to participate in the programme and present proposals for financial support. The Centre is responsible for organising a call for proposals addressing the areas outlined in the Work programme and aligned with the Strategic Agenda.
- **ENISA** to advise the Competence Centre and the Community on research and innovation needs and priorities as per para. 23 of the ECCC regulation and art. 11 of the CSA[67].
- The **Competence Community** to present proposals for research on the topics outlined in this proposal.

[58] https://www.sparta.eu/programs/safair/ last accessed July 2021.
[59] https://civiquantum.eu/ last accessed July 2021.
[60] https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci last accessed July 2021.
[61] https://5g-ppp.eu/wp-content/uploads/2021/06/WhitePaper-6G-Europe.pdf last accessed July 2021.
[62] https://www.esa.int/About_Us/Corporate_news/ESA_ESEC, last accessed July 2021.
[63] https://swe.ssa.esa.int/ssa-space-weather-activities, last accessed July 2021.
[64] https://www.h2020caramel.eu/, last accessed October 2021.
[65] https://www.ai4healthsec.eu, last accessed October 2021.
[66] https://www.humanbrainproject.eu/en/, last accessed October 2021.
[67] ENISA Single Programming Document 2021-2023 outputs 8.4

- **EU bodies and agencies** such as Joint Research Centre (JRC), European Research Council (ERC), European Research Executive Agency (EREA), European Institute of Innovation & Technology (EIT), European Space Agency (ESA), among others.
- The **Quantum Technologies flagship**[68] programme a large-scale initiative pooling resources of research institutions, industry and public funders in this field.
- The EU research community and academia, Alliance for Internet of Things Innovation (AIoTI)[69], European AI Alliance[70], European Internet Forum[71].

Legal frameworks and other areas to take into consideration:

- The Union Rolling Work Programme for European Union cybersecurity certification.[72].
- Artificial intelligence for Europe[73] and AI4EU initiative[74].

Beneficiaries:

- Industry, service providers, researchers, etc.

2.5 ENHANCE EU CYBERSECURITY RESEARCH AND INNOVATION CAPACITIES AND CAPABILITIES

Objectives:

- **Stimulate the production of EU cybersecurity technology (main driver).**
- Promote opportunities for investment in EU Cybersecurity research and innovation.

DEP Impact:

- Ensure alignment with market-driven standards to facilitate industry adoption and global scalability.

ECCC Regulation:

- Article 5 (2)(b)(i)(1): the enhancement of cybersecurity research and innovation, covering the entire innovation cycle, and the deployment of that research and innovation.
- Article 5 (2)(b)(i)(2): the development of cybersecurity industrial, technological and research capacities, capabilities, and infrastructure.
- Article 5 (2)(b)(i)(5): support for the uptake by the market of cybersecurity products, services and processes contributing to the mission set out in Article 3.
- Article 5(2)(b)(ii): supporting the cybersecurity industry, in particular SMEs, with a view to strengthening Union excellence, capacity and competitiveness with regard to

[68] https://qt.eu/ last accessed July 2021.
[69] AIOTI | The Alliance for the Internet of Things Innovation last accessed July 2021.
[70] European AI Alliance | Futurium (europa.eu), last accessed July 2021.
[71] European Internet Forum - Home, last accessed July 2021.
[72] https://digital-strategy.ec.europa.eu/en/library/stakeholder-cybersecurity-certification-group-union-rolling-work-programme-stakeholders-view, last accessed October 2021.
[73] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0237&from=EN, last accessed October 2021.
[74] Home | AI4EU (ai4europe.eu), last accessed July 2021.

cybersecurity, including with a view to connecting to potential markets and deployment opportunities, and to attracting investment.

- Article 5(2)(b)(iii): providing support and technical assistance to cybersecurity start-ups, SMEs, microenterprises, associations, individual experts and civic technology projects;

Overview of the inputs from the Entities

Inputs #32 to #38 highlight the importance of defining strategies for public-private investment in cybersecurity research and innovation and create opportunities for more cybersecurity research uptake.

ENISA views of this proposal

This proposal stems from an ENISA recommendation based on a review conducted of past and present activities performed by the four Pilot Projects and ECSO: ***Accelerate the investment in the development of cybersecurity products and services resulting from EU research activities***.[75]

2.5.1 Implementation of a EU Cybersecurity Research and Innovation Platform

The recommendation underlines the importance of defining strategies and creating conditions that promote the dissemination and exploitation of research and innovation initiatives, reduce the gap between cybersecurity solution producers and the market, attract risk capital from private/public investment and foster collaboration between players. This proposal foresees the preparation of specific policies, guidelines and tools to support the SME, scale-up and start-up community in rapidly developing and producing new products and services.

In this proposal, the ECCC plays a major role as the facilitator of the platform. **The Centre, in collaboration with the Competence Community and other stakeholders such as ENISA, should organise a call for proposals aimed at the implementation of a cybersecurity research and innovation platform to support the work of the wider community during the research and development cycle, until a cybersecurity product or service is produced.**

When the project is finalised, the platform should also interface with the Marketplace presented in the next proposal #7 facilitating a go-to-market process. This proposal considers the following eleven dimensions (list is not exhaustive):

1. The Centre should provide support to projects that encourage public-private investment in research and development and particularly in the generation of innovative cybersecurity solutions. Identify opportunities for investment in start-ups and scale-ups through public-private efforts for larger investment funds.

[75] ENISA recommendations listed in Annex 1 of this document.

2. The Centre should provide support to projects that leverage from the specialisation of Cyber Valleys[76] platforms. Implement a platform that facilitates the cooperation between European regions and encourage the creation of pan-European "Cybersecurity Accelerators" as a network of regional ecosystems. The objective is to expand the research and development of cybersecurity solutions triggered by business partnerships established at regional level.
3. The Centre should provide support to projects that invest in making SMEs cyber secure. A programme targeting SMEs exploring new opportunities and increasing the visibility of innovative companies and projects among financial intermediaries and with the wider investment community. In addition, the program should also facilitate the integration of researchers into the SME ecosystem through entrepreneurial incubation programmes.
4. The Centre should provide support to projects that promote EU cybersecurity champions. Support the growth of EU cybersecurity champions by coordinating and facilitating of merging and growing start-ups.
5. The Centre should provide support to projects that establish an EU Community of investor's in cybersecurity. Build the community by identifying potential investors in cybersecurity and maintain it by keeping a flow of information and specific events to promote business opportunities for investment.
6. The Centre should provide support to projects that promote the development international marketing and business skills, thereby addressing one of the main challenge in the growth of European companies on a global scale.
7. The Centre should provide support to projects that establish strategic priorities for last-mile development, 'productization', marketization of EU cybersecurity products and services.
8. The Centre should provide support to projects that adopt the European Digital and Innovation Hub approach as foreseen in the 'accelerator' scheme of the Digital Europe Programme.
9. The Centre should provide support to projects that implement 'product platforms' managed by flexible Joint Ventures to support specific solutions from single suppliers.
10. The Centre should provide support to projects that promote coordinated research efforts on market analysis to create a mapping of cybersecurity industries and service providers. This analysis will provide a better understanding on the size and extension of the market.
11. The Centre should provide support to projects that help SMEs, start-ups and scale-ups defining go-to-market strategies and develop synergies among community members to aggregate and deliver a unique value proposition for customers and gain a competitive advantage.

[76] https://s3platform.jrc.ec.europa.eu/cybersecurity last accessed June 2021.

2.5.2 Improving EU Cybersecurity research uptake

Europe has a long tradition of research and innovation in various fields. However, many research projects and start-ups lack public/private investment to trigger the next breakthrough innovation. The various actors, including researchers, industry, businesses and entrepreneurs, should collaborate on actionable research, innovation and EU-wide strategic communication on cybersecurity to achieve greater impact.

The objective of this proposal is to promote uptake of EU research and to accelerate the development of cybersecurity products and services resulting from EU research and innovation activities. Europe has a very large pool of talent engaged in cybersecurity research, with only a very small number of products and services being produced in the EU. The low deployment of knowledge assets and research results, production of cybersecurity technology and market uptake are reducing the Union's chances of maintaining the flow of innovation, improving its technological strategic autonomy and being competitive in the global cybersecurity market. It is particularly important to define strategies and create conditions that foster the dissemination and exploitation of research and innovation by reducing the gap between researchers, innovators and cybersecurity producers attracting risk capital from private investment and promoting collaboration. Mediate a healthy and balanced cooperation between the different EU R&I&D actors in the field of cybersecurity, focusing on strategic priorities.

This proposal also focuses on defining a framework and tools to facilitate the transition of research results into development (uptake), production and, at a later stage, into the market.

Theoretical research and the application of research results in demonstration projects are often covered, but the results are not yet industrially ready. With additional funding and the involvement of more end users from industry, results could become industrially-ready.

The collaborative nature of research and innovation requires appropriate management and protection of knowledge and know-how. An important aspect of this framework is the protection of intellectual property rights (IPR) aligned with the rules of participation in EU funding programs such as HE and DEP. The framework should define the requirements to create an environment for researchers and innovators to:

- Disclose knowledge and ideas safely;
- Prove the ownership;
- Profit from commercial exploitation;
- Prevent or discourage its unauthorised use by others.

Baseline:

- **ECSO Cybersecurity Market Radar**[77] was developed with aim to increase visibility of SMEs and large companies. The radar maps more than 200 EU companies at national and

[77] http://www.ecs-org.eu/newsroom/the-latest-edition-of-the-ecso-cybersecurity-market-radar-is-out-now last accessed June 2021.

regional level and a tool for qualitative market analysis to define focussed initiatives and promote EU solutions.

- ECSO will establish a dedicated **'Community of Cyber Investors'**[78] to pool cybersecurity attention and investment from banks, public administrations, corporations, large enterprises, etc. to keep expertise in Europe (in particular to support scale-ups), but also to complement with private funds strategic initiatives also funded by EC and MS.

Actors and contributors:

- The **ECCC,** in collaboration with ENISA and other relevant actors, to organise calls for proposals on one or more dimensions of this proposal in line with articles 5 (2)(b)(i)(1), 5 (2)(b)(i)(2), 5 (2)(b)(i)(5), 5 (2)(b)(ii) and 5 (2)(b)(iii) of the ECCC regulation.
- **ENISA** to contribute to the definition of requirements from the knowledge and experience maintaining the tools for making effective use of the Union's cybersecurity certification framework, market analysis on the main trends in the cybersecurity market on both the demand and supply side, analysis on standardisation gaps and establishment and take-up of European and international standards for risk management in relation to certification.[79]
- The **NCCs** and **Competence Community** to facilitate and present proposals to develop the tools, design and implement the platforms and establish the communities.
- **National competent authorities** in the area of research and innovation.
- **EU bodies and agencies** such as Joint Research Centre (JRC), European Research Council (ERC), European Research Executive Agency (EREA), European Institute of Innovation & Technology (EIT), Executive Agency for SMEs (**EASME**), among others.
- European Digital SME Alliance[80], SMEunited[81], among others entities to provide a contextual and operational perspective to the requirements defined for the call for proposals.

Legal frameworks and other areas to take into consideration:

- EU valorisation policy[82] involves all players and aims to ensure that data, research results and innovation are transformed into sustainable products, processes and services that bring economic value and benefit society.

Beneficiaries:

- Researchers and academics.
- Industry, start-ups and SMEs.
- Investors in cybersecurity.

[78] https://ecs-org.eu/working-groups/cyber-investors-days last accessed June 2021.
[79] ENISA Single Programming Document 2021-2023 outputs 6.4, 7.1 and 7.2
[80] https://www.digitalsme.eu/ last accessed July 2021.
[81] https://www.smeunited.eu/ last accessed July 2021.
[82] https://ec.europa.eu/info/research-and-innovation/research-area/industrial-research-and-innovation/eu-valorisation-policy_en, last accessed October 2021.

2.6 EU CYBERSECURITY MARKETPLACE

Objectives:

- **Stimulate the production of EU cybersecurity technology (main driver).**
- Increase visibility for EU cybersecurity products and services.

HE Impact:

- Strengthened EU cybersecurity capacities and European Union sovereignty in digital technologies.

ECCC Regulation:

- Article 5 (2)(b)(i)(5): support for the uptake by the market of cybersecurity products, services and processes contributing to the mission set out in Article 3.

Overview of the inputs from the Entities

Inputs #43 to #45 highlights the importance of reducing dependence on cybersecurity products and services from third countries and increasing the attractiveness of EU solutions.

ENISA views of this proposal

This proposal stems from an ENISA recommendation based on a review conducted of past and present activities performed by the four Pilot Projects and ECSO: ***Accelerate the investment in the development of cybersecurity products and services resulting from EU research activities***.[83]

The ECCC should organise a call for proposals aiming at bringing together different resources and tools on one platform (Marketplace) for cybersecurity businesses and industries.

The goal of the Marketplace is to help members showcase their solutions, generate new business opportunities, make new contacts and foster cooperation and collaboration between cybersecurity vendors and customers.

This marketplace will also play an important role in promoting cybersecurity tools and services developed under the various EU-funded projects. Apart from Cyberwatching.eu, there is currently no real marketplace specialized in creating new business opportunities for cybersecurity products and services ‘made in EU’. Many companies seek references for cybersecurity products and services from technology vendors, service providers, integrators and consultants. In other situations, decision makers use search engines and news media as a source of information to find a vendor or a provider of cybersecurity products or services. Currently, there is no true

[83] ENISA recommendations listed in Annex 1 of this document.

marketplace with an underlying business model to support the cybersecurity industry to promote its products and services directly to customers.

The Centre should provide support to projects that:

- showcase EU-funded cybersecurity research and innovation projects, cybersecurity products and services offered by EU vendors;
- develop strategies to stimulate and reduce fragmentation of the EU cybersecurity market (demand and supply);
- run promotional campaigns to advertise the marketplace;
- connect with international markets to promote cyber made in EU;
- stimulate measures that close fragmentation of EU market and support 'network effect' through EU community.

Baseline:

- **Cyberwatching.eu**[84] is the European observatory of research and innovation in the field of cybersecurity and privacy. The portal aims at providing unlimited access to SMEs on project information and to a marketplace of new services to help improve their cybersecurity offering.
- **Cybersecurity Market Radar** from **ECSO** for increased visibility of SMEs and large companies, mapping more than 200 EU companies at national and regional level - a tool for qualitative market analysis to define focussed initiatives and promote EU solutions. Business Intelligence dashboard from ECSO.

Actors and contributors:

- The **ECCC** is responsible for attracting the most excellent researchers and innovative enterprises to participate in the programme and present proposals for financial support. The Centre is responsible for organising a call for proposals addressing the areas outlined in the Work programme and aligned with the Strategic Agenda.
- **ENISA** to contribute to the definition of requirements based on the knowledge and expertise from the work developed on market analysis and main trends in the cybersecurity market, both on the demand and supply side.[85]
- The **Competence Community** to present the proposals for the design and development of the methods and tools considered for the Marketplace.
- **EU bodies and agencies** such as Executive Agency for SMEs (**EASME**), among others.
- European Digital SME Alliance[86], SMEunited[87], among others entities.

[84] https://cyberwatching.eu/ last accessed July 2021.
[85] ENISA Single Programming Document 2021-2023 output 7.1.
[86] https://www.digitalsme.eu/ last accessed July 2021.
[87] https://www.smeunited.eu/ last accessed July 2021.

Beneficiaries:

- EU cybersecurity businesses and industry.

2.7 COMPETENCE COMMUNITY COLLABORATIVE NETWORKS

Objectives:

- **Supporting European Cybersecurity cooperation structures, approaches and actors (main driver).**
- Promote collaboration between members of the Competence Community.

ECCC Regulation:

- Article 5 (2)(f): facilitating collaboration and the sharing of expertise among all relevant stakeholders, in particular members of the Community.

Overview of the inputs from the Entities

Inputs from #48 to #52 highlight the importance of having a mobilised and engaged Competence Community as well as to promote collaboration between members and display the results from ECCC-funded projects.

ENISA views of this proposal

This proposal stems from an ENISA recommendation based on a review conducted of past and present activities performed by the four Pilot Projects and ECSO: **Capitalise on the results of EU funded projects.**[88] The four Pilot Projects and ECSO in their Research focus areas document also noted the need for “efficient and sustainable collaboration among variety of organisations build on solid understanding of requirements, designing and implementing effective norms and models, and the supporting infrastructure.”

The Competence Community is multi-layered group of entities and individuals specialized in cybersecurity with a sectoral (automotive, aerospace, finance, etc.), local (Member States), sub-regional and regional (EU) perspective. A community with different tiers of engagement and scopes. Defined as a diverse group, the Competence Community is supposed to attract members from the academia, industry, businesses, professionals, researchers, Digital Innovation Hubs and entrepreneurs with one theme in common: cybersecurity.

The ECCC should organise a call for proposals aiming at the implementation of a platform and the organisation of initiatives that contribute to the effective mobilisation and engagement of the Competence community.
The Centre should support projects that:

[88] ENISA recommendations listed in Annex 1 of this document.

- Organise matchmaking events to promote networking and develop synergies with Community members at the regional, national and EU level.
- Establish a sub-community of Digital Innovation Hubs focused on cybersecurity and providing services such as the Cyber-Valleys[89] project. Coordinate and align activities between different Digital Innovation Hubs working in the field of cybersecurity.
- Implement sub-community structures or chapters at sectoral and vertical levels.
- Implement a dashboard showing the execution of Competence Centre funds. The aim is to provide visibility on the areas, projects, sectors, entities, etc. benefiting from the Competence Centre funds.
- Encourage the clustering of projects into different groups (e.g. categories of research areas) to promote cooperation.
- Provide strategic oversight capabilities to cater for continuous monitoring and evaluation of activities.
- Promote seamless integration with other platforms and in particular the ones proposed in this document such as research and innovation platform and EU cybersecurity marketplace.

Baseline:

- The Entities explored several opportunities to closely cooperate and coordinate activities. The idea behind the European **Cybersecurity Competence Network**[90] formed by the four Pilot Projects aimed at exploring the different but complementary approaches to shared and common goals. The main areas of focus include cyber ranges, education, governance, road mapping and threat intelligence. However, many other areas could have been considered to avoid duplication of efforts, promote optimisation and develop synergies between Entities.
- The European **Cybersecurity Atlas[91]**, a digital knowledge management platform, aims to map, categorise and stimulate collaboration between entities with cybersecurity expertise across Europe.
- The **AI REGIO**[92] innovation action aims to consolidate the collaboration in the pan-European network of Digital Innovation Hubs (DIHs) by enhancing the offering of regional DIHs to manufacturing SMEs on three levels: Policy impact; technological impact and business impact.

[89] https://cyber-valley.de/, last accessed June 2021.
[90] https://cybercompetencenetwork.eu/, last accessed June 2021.
[91] https://cybersecurity-atlas.ec.europa.eu/, last accessed October 2021.
[92] https://www.airegio-project.eu, last accessed October 2021.

Actors and contributors:

- The **ECCC** is responsible for attracting the most excellent researchers and innovative enterprises to participate in the programme and present proposals for financial support. Article 5 (2)(f) of the Regulation states that the Centre should facilitate collaboration and the sharing of expertise among all relevant stakeholders, in particular members of the Community.
- **ENISA** to provide relevant expertise to the ECCC on Community mobilisation and engagement (art. 8(2) of the ECCC regulation, ENISA strategic objective #SO1 and activity 9 of ENISA SPD 2021-2023).
- The **ECCC** to pool investment in the development of the tools required for mobilising and engaging the Competence Community;
- The **Competence Community** to present the proposals for the design, development and implementation of the proposed Competence Community platform and other relevant tools.

Beneficiaries:

- Members of the Competence Community.

2.8 FOSTER THE HUMAN AND SOCIAL DIMENSION IN CYBERSECURITY

Objectives:

- **Introduce a human and societal perspective in cyber (main driver).**
- Create expertise in human and social sciences for cybersecurity.
- Increase awareness on cybersecurity threats with EU SMEs and Citizens.

ECCC Regulation:

- N/A – Crosscutting topic.

Overview of the inputs from the Entities

Inputs #54 and #55 highlight the importance of Improving the EU citizen’s digital lives and serving as a guidance to moral daily living.

Moreover, the Input #27 highlights the need to organise regular communication campaigns to promote 'Cyber Secure EU citizen' and SMEs.

ENISA views of this proposal

This proposal stems from an ENISA recommendation based on a review conducted of past and present activities performed by the four Pilot Projects and ECSO: ***Incorporate the human and societal dimensions into cybersecurity.***[93]

The ECCC should organise a call for proposals to support the research on the importance of having a human and social dimension in cybersecurity, contributing to the protection of EU values and fundamental rights (freedom, equality, rule of law, human rights, human dignity and democracy) in the digital space.

It also in the scope of this proposal the organisation of initiatives and activities to transpose these dimensions into concrete actions. Furthermore, the European Commission proposed two legislative initiatives to upgrade rules governing digital services in the EU. The Digital Services Act and Digital Markets Act[94] aim to create a safer digital space where the fundamental rights of users are protected and to establish a level playing field for businesses. The following list provides (not limited to) eight dimensions to this proposal. The Centre should provide support to projects that:

1. Research the importance of a having human and social dimension in cybersecurity, contributing to the protection of EU values and fundamental rights (freedom, equality, rule of law, human rights, human dignity and democracy) in the digital space;
2. Include a human and social dimension aiming at the protection of EU values and fundamental rights in cyberspace;
3. Establish ethics focus groups to look at broader cross-sectoral and cross-technology issues, such as fairness and inclusiveness;
4. Produce knowledge on European doctrines for digital openness, transparency, liability and accountability;
5. Research on privacy-enhancing technologies (PET). Develop practices and tools that support users in preserving online privacy. Research should ensure that users can easily enforce regulations such as the GDPR;
6. Research and develop solutions on cybersecurity methods and tools that actually meet users' needs and support their activities, rather than acting as a barrier to productivity;
7. Research on security visibility. Design user interfaces and interactions that end users actually see and that help them adopt actual behaviours;
8. Research on social engineering and human error in cybersecurity. Develop examples and methods that effectively provide new insights into how people interact with each other in social media and other online mechanisms to avoid common mistakes that lead to system compromise;
9. Research and development of innovative solutions to increase effectiveness in raising awareness. Repetition is the key to breaking habits and changing behaviours. Awareness-

[93] ENISA recommendations listed in Annex 1 of this document.
[94] https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package last accessed

Raising-as-a-Service is a tool based on the experience and lessons learned from previous campaigns to automate the process of running an awareness campaign. Social media is the most efficient media for this type of service. One of the advantages is the possibility to evaluate the reach, engagement and interaction of an awareness campaign.

Baseline:

- **ENISA** develops assessments (Article 9 of the CSA) and contributes to various initiatives that brings a human and societal dimension to cybersecurity. The Agency also coordinates the European Cybersecurity Month (ECSM)[95], the Union's annual campaign dedicated to promoting cybersecurity among EU citizens and organisations, and to providing up-to-date online security information through awareness raising and sharing of good practices.
- **Women4Cyber[96]** is a non-profit European private foundation with the objective to promote, encourage and support the participation of women in the field of cybersecurity.
- **SPARTA** is currently working on a method to assess and improve 'societal readiness' from an early development phase and ECHO conducted an societal impact assessment.
- **ECSO** organises the Youth4Cyber[97] initiative aiming at educating and raising the awareness of young people (6 to 26-year olds) on cybersecurity.
- **CyberSec4Europe** is currently working on methodologies to improve user awareness of security.
- **SPARTA** developed strategies for cybersecurity communication & dissemination and is currently working on campaigns for various target groups such as high schools and SMEs.
- **SHERPA**[98] project investigates, analyses and synthesises an understanding of the ways in which smart information systems (SIS; the combination of artificial intelligence and big data analytics) impact ethics and human rights issues. It will develop novel ways of understanding and addressing SIS challenges, evaluate with stakeholders, and advocate the most desirable and sustainable solutions.
- The **CANVAS[99]** project ensure that the future generation of cybersecurity experts obtains basic insights into and knowledge of how to tackle ethical and legal dilemmas in cybersecurity.

Actors:

- The **ECCC,** in collaboration with ENISA and other relevant actors, is responsible for attracting the most excellent researchers and innovative enterprises to participate in the programme and present proposals for financial support. The Centre is responsible for

[95] https://cybersecuritymonth.eu/ accessed July 2021.
[96] https://women4cyber.eu/ last accessed July 2021.
[97] https://ecs-org.eu/initiatives/youth4cyber last accessed July 2021.
[98] https://www.project-sherpa.eu, last accessed October 2021.
[99] https://canvas-project.eu/, last accessed September 2021.

organising a call for proposals addressing the areas outlined in the Work programme and aligned with the Strategic Agenda.

- The **NCCs** and **Competence Community** to facilitate and present proposals to develop the tools, the design and implement the platforms and establish the communities.
- **EU bodies and agencies** such as Fundamental rights agency (FRA).

Beneficiaries:

- Digital civil society.

3. CLOSING REMARKS

This study highlights some of the main needs that are also considered priorities by the members of the four Pilot Projects, ECSO, ENISA and the EC in order to grow cybersecurity research, development and innovation (RDI) in Europe. The eight proposed areas focus will require public and private investment due to the nature and scope of the initiatives. The main goal of this study is to discuss these proposals with the ECCC Governing Board (EC and Member States) in the context of the preparation of the Strategic Agenda and the Multiannual Work Programme and to highlight future cybersecurity investment needs and priorities. The ECCC mandate will be in place until 2029 and ENISA will continue to provide advice on its own views and understanding of RDI needs and priorities, in line with the Centre's Regulation and Article 11 of the Cybersecurity Act. This is the first edition of an annual report that ENISA will produce in collaboration with stakeholders and members of Cybersecurity Competence Community.

ANNEX 1 – REVIEW OF PAST AND ONGOING ACTIVITIES

In a previous study named ‘An overview on activities performed by Pilot Projects and ECSO’, ENISA presents an analysis on the activities performed by the Entities during their first two years of activity in specific areas. The recommendations produced in this study are as follows:

1. **Accelerate the investment in the development and production of cybersecurity products and services resulting from EU research activities**. Europe has a very large pool of talent working in cybersecurity research, but a very small number of products and services ‘made in the EU’. Low market uptake and low deployment of knowledge assets and research results reducing the Union’s chances of maintaining the flow of innovation, improving its technological strategic autonomy and being competitive in the global cybersecurity market. ENISA see research adoption results as one of the least addressed topics by the Entities, considering the limited number of results reported. It is particularly important to define strategies and create conditions that encourage the dissemination of research and innovation by reducing the gap between researchers, industry and market participants (entrepreneurs and businesses), attracting venture capital from private investment, and promoting collaboration. ENISA recommends the development of tools and processes to facilitate the transition of research assets into development and, at a later stage, into production. Specific policies, guidelines and tools should be available to support the start-up community in rapidly developing and producing new cybersecurity products and services. A cybersecurity innovation observatory could help identify and promote opportunities for research uptake. A marketplace where researchers can present their results, start-ups can display their products and businesses attract venture capital along with other initiatives to foster cooperation and collaboration between cybersecurity actors and market players.

2. **Consolidate a vision for the development of cybersecurity competencies across EU communities.** From the information provided, there is a need for better alignment and coordination of EU funded programs and Projects to avoid overlaps and duplication between Entities. ENISA recommends a balanced and focused approach in selecting the topics and areas based on the specific priorities and needs of the EU Member States. ENISA see coordination between EU communities as key priorities for the future European Cybersecurity Competence Centre and National Coordination Centres. The future Cybersecurity Competence Community will be responsible for the implementation of EU funded projects and initiatives during the next Multiannual Financial Framework (2021-2027)[100]. Coordination will be under the responsibility of the Competence Centre and ENISA will play a role as per the regulation by ensuring that there is

[100] https://ec.europa.eu/info/strategy/eu-budget/long-term-eu-budget/2021-2027/documents_en, last accessed June 2021.

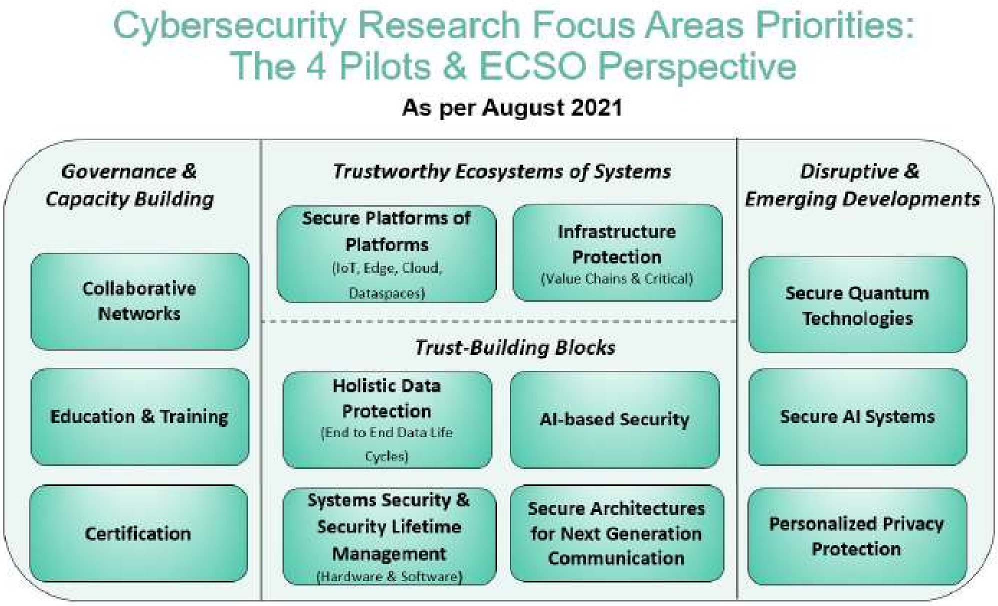
complementarity and avoiding overlaps with the work of the Agency and other EU actors in the field of cybersecurity.

3. **Incorporate the human and societal dimensions into cybersecurity**. Debating the importance of the human and societal dimensions of cybersecurity will contribute to the protection of EU values and fundamental rights (freedom, equality, rule of law, human rights, human dignity and democracy) in the digital space. Future EU funded cybersecurity projects should necessarily include human and societal dimension to promote the protection of EU values and fundamental rights in cyberspace. Moreover, innovation does not always stem from the technical dimension - social innovations helps to address societal challenges posed by digitisation and the use of cyberspace. These and other issues related to the human and societal dimension should take into account in future research work of the Competence Community.

4. **Capitalise on the results of EU funded projects.** Using results as a starting point and impact as a baseline will help shape future project proposals from the Competence Community. The aim is to avoid future EU funded projects starting from scratch zero and not to waste the efforts and results of these Entities. In addition, the Competence Community and projects should benefit from the experience of the four Pilot Projects and ECSO and incorporate lessons learned, as stated in paragraph 17 of the CCCN regulation[3]. For example, a platform and database of qualitative information, impacts and lessons learned from past and ongoing activities of the different EU actors could serve as a valuable resource for proponents of future EU activities. Another recommendation is to introduce a tool to consolidate all the platforms developed by these entities. For example, consolidating many existing cyber ranges and other research infrastructures into one federated platform will allow for greater efficiency (creation of compatible use cases) and reduce the fragmentation of technological solutions available in this area.

ANNEX 2 – INPUTS AND R&D FOCUS AREAS FROM THE ENTITIES

The four Pilot Projects and ECSO road-mapping Focus Group prepared in August 2021 a consolidated cybersecurity agenda pinpointing research challenges of high-priority for the EU. The figure below depicts the selected areas, in no particular order, seen as most notable yet non exhaustive areas of focus.


Cybersecurity Research Focus Areas Priorities: The 4 Pilots & ECSO Perspective

As per August 2021

Governance & Capacity Building
Collaborative Networks
Education & Training
Certification
Trustworthy Ecosystems of Systems
Secure Platforms of Platforms (IoT, Edge, Cloud, Dataspaces)
Infrastructure Protection (Value Chains & Critical)
Trust-Building Blocks
Holistic Data Protection (End to End Data Life Cycles)
AI-based Security
Systems Security & Security Lifetime Management (Hardware & Software)
Secure Architectures for Next Generation Communication
Disruptive & Emerging Developments
Secure Quantum Technologies
Secure AI Systems
Personalized Privacy Protection

The four pilots and ECSO also provided their views on the way forward during the exercise organised by the EC with the support of ENISA. The inputs generated by the Entities for this exercise are listed in the table below.

#	Topic	Proposal	Baseline	Actors	Beneficiaries	Benefits/Impact
1	Cyber infrastructure	Develop and promote the adoption of a common EU-wide cyber threat intelligence taxonomy and machine-readable format for the classification and exchange of threat information	ENISA and JRC Taxonomies, SPARTA T-SHARK	ENISA; Competence Community	Industry; Businesses; Organisations	Offers automatized and harmonised CTI sharing process
2	Cyber infrastructure	Design and implement an online-platform for sharing knowledge and tools made in the EU (Cyber resource centre)	Four Pilots and ECSO Websites and Platforms	CCCN	Businesses; Citizens; Organisations	Organises and structures the EU offering of cyber defence tools
3	Threat based defence	Define and promote the adoption of a common EU-wide method for the design and development of cyber-resilient software and system architectures	CS4EU Framework	Competence Community	Industry; Businesses	Increases the software and systems resilience to cyberattacks
4	Approaches and methods for cybersecurity assessments, mitigation measures and maturity evaluations	Define a common EU cybersecurity maturity assessment and evaluation framework	CMAF	ENISA; Competence Community	Industry; Businesses	Increases trust and introduces harmonisation of the assessment process
5	Approaches and methods for cybersecurity assessments, mitigation measures and maturity evaluations	Design and develop automated cybersecurity assessment tools (evaluates cyber risk exposure and proposes mitigation measures)	RASEN	CCCN	Businesses; Organisations ; Citizens	Increases efficiency and automation of the security assessment process
6	Threat landscape and analysis	Produce independent, sectoral, thematic and multipurpose cyber threat landscapes	ENISA ETL	ISACs; ENISA; CCCN	Sectors; Industry	Improves the knowledge about threats affecting certain sectors/industries
7	Trust in technology	Develop a methodology and standards for secure system engineering (SDLC)		Competence Community	Industry	Reduces the chances of exploitation and increases trust in the technology
8	Trust in technology	Implement an online-platform for trustworthy and verified hardware and software	EU Certification Schemes	Member States; European Commission; ENISA; CCCN	Industry; Businesses; Organisations ; Citizens	Increases trust in the EU Digital Single Market through certification of ICT products, services and processes
9	Policy initiatives	Define a model for evidence-based policymaking in cybersecurity	ECHO E-MAF	ENISA; European Commission; NIS-Cooperation Group	Policy makers	Better informed decisions based on evidence.
10	Policy initiatives	Prepare vendor certification mechanisms for digital supply-chain security		Member States; European Commission; ENISA	Operators of Essential Services; Industry	Increases trust and helps identifying responsibilities and requirements across the supply chain of complex ICT systems

11	Vulnerability management	Define a framework and implement platform to handle the disclosure, consolidation and maintenance of software and hardware vulnerability information	Zerodisclo, VARIoT	ENISA; Competence Community	Industry; Businesses	Increases the software and systems resilience to cyberattacks
12	Approaches and methods for cybersecurity assessments, mitigation measures and maturity evaluations	Define a method to evaluate and measure the resilience of an operator of essential services technical architecture		ENISA; Competence Community	Industry; Businesses	Allows the preparation of resilience improvement plans
13	Approaches and methods for cybersecurity assessments, mitigation measures and maturity evaluations	Define a method and develop tools for supply-chain security assessments, evaluations and testing		ENISA; CCCN	Industry; Businesses	Increases the efficiency in security assessments of the digital supply chain
14	NIS directive implementation	Develop self-assessment tools, methods and standards in support of the NIS Directive implementation		ENISA; European Commission; NIS-Cooperation Group	Operators of Essential Services	Harmonises the processes and methods for OES
15	Supply-chain resilience	Define incident reporting requirements for digital supply chains		ENISA; Competence Community	Industry; Businesses	Improves the response to cyberattacks across digital supply chains
16	Incident management (detection, analysis, reporting and response)	Design and develop a common EU early warning system for operators of essential services	ECHO EWS	CSIRTs Network; ENISA; CCCN	Operators of Essential Services	Increases the efficiency in the response to cross-border cyber threats
17	Incident management (detection, analysis, reporting and response)	Define emergency mechanisms to promote cooperation among entities affected by cross-border cybersecurity incidents		CSIRTs Network; ENISA; CCCN	CERTs; Emergency Response	Increases the efficiency in the response to cross-border cyber threats
18	Policy initiatives	Establish standards for incident reporting harmonisation across the EU (NISD entities, CIRTSs)		CSIRTs Network; ENISA; European Commission	Operators of Essential Services	Improves the response to cyberattacks
19	Cyber infrastructure	Develop and implement federated and open-source cyber ranges, cyber arenas and training online-platforms	CYBERWISER.EU	CCCN	Industry; Businesses	Consolidates the offering of cyber ranges and training platforms and technology
20	Cyber infrastructure	Define and maintain a EU cybersecurity competency map including service and solution providers, consultants, integrators, developers, among others	European Cybersecurity Atlas	JRC; ENISA; CCCN; Competence Community	Industry; Businesses; Organisations	Offers one consolidated view over all EU cyber competencies
21	Cyber infrastructure	Implement a EU online-platform for cybersecurity researchers (integrated with other research platforms and CCCN platforms)		JRC; CCCN;	Researchers; Institutes	Promotes research knowledge sharing and development of synergies within the research community
22	Higher education	Implement a one-stop platform for cybersecurity in higher education (mapping tool, requirements, industry corner, etc)	CYBERHEAD	CCCN; Competence Community; ENISA	Universities; Citizens	Promotes interest on cybersecurity higher education and help identifying gaps

23	Professional training and careers in cyber	Organise specialised programs in cybersecurity professional training at a local, sectoral and regional level	4 Pilots Training Programs	Competence Community	Industry; Businesses; Organisations	Adjusts cybersecurity training offerings to market needs and requirements
24	Professional training and careers in cyber	Organise joint exercises with public, defence and security authorities		EDA; EUROPOL (EC3); ENISA; CCCN; European Commission; JCU	EU Institutions; Competence Community	Establishes synergies and coordination between the cybersecurity civilian and defence spheres
25	Cyber skills	Organise an annual European forum on the development of Cybersecurity Skills (CSF)		EDA; EUROPOL (EC3); ENISA; CCCN; European Commission; JCU	EU Institutions; Competence Community	Promotes the continued assessment of required EU cyber skills and discussion on how to develop
26	Higher education	Rollout the European Cybersecurity Skills Framework (CSF)		ENISA; CCCN; Competence Community	Competence Community	Increases the adoption of the EU Cybersecurity Skills Framework
27	Cyber awareness	Organise regular communication campaigns to promote a 'Cyber Secure EU citizen' and SME	ECSM	Member States, European Commission; ENISA; CCCN; Competence Community	Citizens; SMEs	Raises awareness on cyber threats and promote cyber hygiene and cybersecurity best practices
28	Research, development and innovation	Research the security for digital solutions in mobility (people and goods), smart cities, smart governments and space		Competence Community	Industry; Businesses	Mitigates the risks with digital solutions in mobility
29	Research, development and innovation	Research the security of AI algorithms (Life-cycle), Biotechnology, NextGenInternet, etc.	ENISA AI-TL, SPARTA SAFAIR	Competence Community	Industry; Businesses	Mitigates the risks during the different AI development life-cycle stages
30	Research, development and innovation	Research the security of machine-to-machine communication (including IoT, ICS, robotics, etc.) for strategic verticals to the EU economy/industry		Industry; Competence Community	Industry; Businesses	Secures M2M Communications including IoT and ICS
31	Research, development and innovation	Define approaches and strategies to identify and address emerging cybersecurity challenges and threats (quantum computing, 6G, etc.)	ENISA Foresight Program; ECSO SRIA; SPARTA road map; CS4EU SRIA	European Commission; JRC; ENISA; EC3; EDA; JCU; ECSO; Competence Community	Industry; Businesses	Identifies strategies to mitigate the risks introduced with the adoption of emerging technologies
32	Cybersecurity research results uptake	Develop strategies to facilitate the transitioning from research results into development		CCCN	Researchers; Institutes; Industry	Increases the number of new cybersecurity products and services

						generated from EU research
33	Cybersecurity research results uptake	Implement a cybersecurity innovation observatory for the next generation of cybersecurity products and services	Cyberwatching.eu	CCCN; Competence Community; ENISA	SMEs; Start-ups; Scale-ups	Generates more opportunities for innovation in cybersecurity
34	Research, development and innovation	Define computational security models in the areas of cryptography, authentication and key exchange		Competence Community	Industry	Increases the security of software, systems and networks
35	Policy initiatives	Introduce regulatory support for innovative business models in cybersecurity		European Commission; ENISA; ECSO	Industry; SMEs; Start-ups; Scale-ups	Increases the EU Cybersecurity Industry attractiveness for internal and external investment
36	Start-ups and scale-ups (SMEs)	Establish an organisation of EU cybersecurity champions		CCCN	SMEs; Start-ups; Scale-ups	Promotes a business culture in the EU cybersecurity market and provides visibility to EU SMEs
37	Investment and funding strategies	Define a strategy for public-private investment in cybersecurity research and innovation		European Commission; ECSO	SMEs; Start-ups; Scale-ups	Increases the number of public-private projects
38	Investment and funding strategies	Implement an 'investors in cybersecurity innovation' online-platform	ECSO funds-of-funds proposal and Cyber investors days	CCCN	Industry	Generates more opportunities for funding in cybersecurity projects
39	Cybersecurity market	Define a cybersecurity products and services catalogue and offering		CCCN; ECSO; ENISA	Industry	Reduces fragmentation and strengthens the position from vendors
40	Go-to-market strategies	Define a competitive cybersecurity value chain		CCCN; ECSO; Competence Community	Industry	Reduces fragmentation and strengthens the position from vendors
41	Go-to-market strategies	Implement EU incubators and accelerators (virtual and physical)	Cube5; Station F	CCCN	SMEs; Start-ups; Scale-ups	Stimulates the growth of cybersecurity start-ups
42	Go-to-market strategies	Define go-to-market strategies for cybersecurity products and services	ECSO Made in EU label	CCCN; ECSO; Competence Community	SMEs; Start-ups; Scale-ups	Enhances the overall customer experience and stimulates the demand
43	Cybersecurity market	Produce an independent annual market analysis of the cybersecurity landscape in Europe	ECSO Market Radar; ECHO Market Analysis Report	ENISA; CCCN; ECSO	SMEs; Start-ups; Scale-ups	Provides independent information about the market in the EU

44	Cybersecurity market	Define a EU strategy to stimulate the cybersecurity market (demand and supply)		CCCN	SMEs; Start-ups; Scale-ups	Reduces the dependency on cybersecurity products and services from 3rd countries
45	Cybersecurity market	Design and implement a platform supporting the EU cybersecurity marketplace	ECSO Matchmaking	CCCN	Competence Community	Increases the attractiveness, competition, customer acquisition, promotion, presence, among others
46	Policy initiatives	Prepare policy proposals to improve the EU technological autonomy in cybersecurity		European Commission; ENISA; ECSO; Competence Community	Operators of Essential Services; Industry	Reduces the dependency on cybersecurity products and services from 3rd countries
47	Policy initiatives	Define a rule of origin criteria in the procurement of technology supporting critical infrastructure		European Commission	Industry; SMEs; Start-ups; Scale-ups	Reduces the dependency on cybersecurity products and services from 3rd countries
48	Competence Community	Define the Competence Community value proposition		NCC; European Commission	Competence Community	Increases the attractiveness of the Competence Community
49	Competence Community	Define a membership model for the Competence Community		NCC; European Commission	Competence Community	Increases mobilisation, transparency and harmonisation of criteria for community membership
50	Competence Community	Implement a Competence Community online-platform	Cyber Competence Network	CCCN	Competence Community	Serves as a resource centre, promotes the development of synergies between members and a display for projects
51	Competence Community	Organise Competence Community annual events (online and virtual)		CCCN	Competence Community	Promotes the development of synergies between members
52	Competence Community	Define a Competence Community governance model	ECHO Governance White Paper	CCCN	Competence Community	Improves the efficiency and control of the community, as well as communication and engagement of stakeholders

53	National Coordination Centres	Implement a online-platform to support the Network of National Coordination Centres		CCCN	National Coordination Centres	Promotes knowledge, experience and information sharing, as well as development of synergies among NCCs
54	EU values and fundamental rights in cyberspace	Promote the protection of EU values in the digital space compromised by cyber threats		European Commission; ENISA; Competence Community	Citizens	Improves EU citizens digital lives
55	EU values and fundamental rights in cyberspace	Introduce the cybersecurity perspective in a EU digital ethics committee		European Commission; ENISA; Competence Community	Citizens	Serves as a guide to moral daily living
56	User aspects	Contribute to a EU digital citizenship model from a cybersecurity perspective		European Commission; ENISA; Competence Community	Citizens	Improves the confidence and promotes a positive engagement of citizens with digital technologies
57	User aspects	Define a privacy guarantee model	CS4EU and SPARTA	European Commission; ENISA; Competence Community	Businesses; citizens; organisations	Complements the GDPR by providing additional tools to monitor and control the access to personal data
58	Policy initiatives	Adoption of a EU-wide electronic ID-based trust framework and schemes	CEF eID; eIDAS;	European Commission	Businesses; citizens; organisations	Harmonises the electronic identification of citizens and organisations across the Union
59	Policy initiatives	Define an industry liability model for cybersecurity software and services		European Commission; ENISA; Competence Community; ECSO	Businesses; citizens; organisations	Reduce the risks introduced by defective software.

XX-00-00-000-XX-X

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 000-00-0000-000-0
doi: 0000.0000/000000