ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

Strategic Agenda

March 2023

ECCC – Strategic Agenda

March 2023

Introduction

The digitalisation of the European economy and society and the growing number of incidents in cyberspace has become even more challenging with the Russian war against Ukraine, which exacerbates the importance of a cohesive European cybersecurity strategy and coordinated actions to further strengthen the Union's resilience and ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from cyber incidents. An approach designed to provide an open, free, stable and secure cyberspace that can be trusted by citizens making use of digital tools and services is needed, with full respect for fundamental rights. Paving the way towards contributing to the European Union, global leadership in cybersecurity implies significant alignments of EU investments in cybersecurity research, innovation and industrial developments. Therefore, it would provide grounds for boosting the European cybersecurity competitiveness and support the growth of the European Cybersecurity Competence Community. This includes strengthening the cybersecurity maturity of the European industrial base, as well as developing the right competencies and skills.

The European Cybersecurity Competence Centre (ECCC) provides a unique opportunity to define a vision for the EU investment in cybersecurity. The ECCC is in charge of developing and monitoring the implementation of the Strategic Agenda[1] which is "*a comprehensive and sustainable cybersecurity industrial, technology and research strategy which sets out strategic recommendations for the development and growth of the European cybersecurity industrial, technological and research sector and strategic priorities for the Competence Centre's activities and is not binding with respect to decisions to be taken on the annual work programmes* "[2].

The Strategic Agenda ('Agenda') should set up goals to be achieved by investing in ambitious and specific projects that will *"strengthen the EU leadership and strategic autonomy, support Union technological capacities and increase the global competitiveness of the Union's cybersecurity industry"*[3] through the promotion of research, innovation and industrial development in the area of cybersecurity.

The Agenda's goal is to create a unified and common vision to the EU investment in cybersecurity required to fulfil the objectives set in the EU Cybersecurity Strategy[4] and in the ECCC Regulation 2021/887 ('the Regulation')[5]. By aligning the investment priorities of the EU and of the Member States, the Agenda contributes to achieving greater impact and provides an incentive for national

[1] REGULATION (EU) 2021/887 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, Article 5.

[2] REGULATION (EU) 2021/887 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, Article 2 (8).

[3] REGULATION (EU) 2021/887 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, Article 3.

[4] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade

[5] REGULATION (EU) 2021/887 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres

investment in cybersecurity. The Agenda reflects a holistic view of cybersecurity investment priorities, incorporating the views from important groups of stakeholders and users, such as research and academia, the cybersecurity industry with a strong focus on SMEs and startups, public authorities or operators of essential and important infrastructures per the Network Information Security (NIS) 2 Directive.

The tasks will be carried out on the basis of relevant Union financial resources, namely identified as the Digital Europe Programme (DEP) and for joint actions Horizon Europe (HE) - the Framework Programme for Research and Innovation and contributions from Member States.

The Agenda refers both to strategic and implementation tasks of the ECCC. The implementation tasks range from implementing other programmes where provided for in the relevant acts of the Union, to improve "*synergies and coordination between the cybersecurity civilian and defence spheres by facilitating the exchange of (i) knowledge and information with regard to dual-use technologies and applications; (ii) results, requirements and best practices; and (iii) information with regard to the priorities of relevant Union programmes.*"[6] The latter implementation task is justified considering the rapid evolving geopolitical context in Europe due to the conflict in Ukraine. Although dialogue could be put in place between the ECCC and the European Defence Agency (EDA) on how to create these synergies – as stated by the Joint Communication on EU Cyber Defence policy[7], the ECCC is not entitled to manage defence fundings.

Although the Agenda is not binding with respect to the decisions taken on the annual work programmes of the ECCC, the implementation of the respective funds should be done in accordance with the Agenda. This provision underlines the importance of this document, which extends beyond the ECCC and the Network of National Coordination Centres (NCCs) (the 'Network') itself and also touches upon research and innovation funding instruments such as the DEP and HE.

Policy landscape

The establishment of the ECCC is taking place in a dynamic cybersecurity political context, including several initiatives at EU level. In addition to the contextual situation the EU as mentioned in the introduction, the EU should foster the development of competencies, skills, infrastructures and competitiveness in emerging areas identified in the EU's Cybersecurity Strategy for the Digital Decade. To do so, the EU should rely on a strong industrial base which will require significant investments to allow the Union to become a global leader in cybersecurity and strengthen the cybersecurity maturity of the EU industrial base.

According to the regulation, the ECCC will implement the cybersecurity component of the DEP with operation objectives, as defined in the Regulation, establishing the ECCC and the Network. Synergies should be made with other specific objectives of DEP, where cybersecurity is also funded, like for example Advance Digital Skills**.** The five specific objectives[8] in the DEP are distinct but interdependent. Furthermore, the DEP Regulation[9] introduces European Digital Innovation Hubs

[6] REGULATION (EU) 2021/887 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, Article 5.3.g.

[7] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL EU Policy on Cyber Defence, JOIN(2022) 49 Final.

[8] Specific Objective 1- High Performance Computing; 2 – Artificial Intelligence 3 – Cybersecurity and Trust; 4 – Advanced Digital Skills; 5 – Deployment and Best Use of Digital Capacities and Interoperability

[9] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0694

(EDIHs), and the NCCs should align its activities with EDIHs to reach synergies and avoid duplication of efforts.

At the present time, the ECCC is responsible for the implementation of joint actions receiving support under the provisions that relate to cybersecurity in Horizon Europe. Given the ECCC's role and function, it is worthwhile to explore in the future whether this scope can be widened to include broader implementation of (civil) cybersecurity funding across DEP and HE.

The ECCC aims to foster the Union's resilience to cybersecurity incidents and ability to face and respond to those events, including tackling cybercrime activities. As a priority and for the duration of its mandate, the ECCC could be involved in supporting the implementation of specific policies, such as:

- actions foreseen in the **EU's Cybersecurity Strategy for the Digital Decade.**
- the NIS and **NIS2 Directive.** As a result, the ECCC would contribute to invest in projects that will take part in raising the EU common level of ambition on cybersecurity, through a wider scope, clearer rules and stronger supervision tools.
- the **European Cybersecurity certification schemes** as foreseen in the Cybersecurity Act, as there is a need for a more harmonisation of the schemes, while using a market-driven approach to increase trust in cybersecure ICT technologies, services and processes.
- the **Cyber Resilience Act** (CRA). On the basis of the requirements of the regulation, the ECCC could support implementation of the CRA especially in relation to the SMEs.
- facilitating the implementation of the **5G Toolbox**[10].

Apart from defining the priorities it is also important to take into consideration the targets to be achieved by 2030 established in the **Digital Compass for the EU's digital decade**, including skills, secure and sustainable digital infrastructures, digital transformation of businesses and digitalisation of public services. The targets are further defined in the policy programme **Path to the Digital Decade**, where one of the general objectives of the Digital Decade Policy Programme 2030 is *"improving resilience to cyberattacks, contributing to increasing risk-awareness and the knowledge of cybersecurity processes, and increasing the efforts of public and private organisations to achieve at least basic levels of cybersecurity"*[11]***.***

The ECCC will take into account and promote full respect for fundamental rights when implementing the Union's digital development for the next decade, including the rights and principles adopted by the **European Declaration on European Digital Rights** and **Principles for the Digital Decade**[12].

While seeking for synergies between the ECCC and EDA regarding "*the assessment of critical cyber technologies*", it is essential to take into consideration the **Security Union Strategy 2020-2025**, the

[10] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Secure 5G deployment in the EU - Implementing the EU toolbox, COM(2020) 50 final.

[11] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

[12] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0028

EU strategy to tackle organised crime 2021-2025[13], the **Strategic Compass**[14] and the **Joint communication for a European cyber defence policy**[15] and relevant Council conclusions and positions reacting to the policies and strategies written by **the Commission or European External Action Service (EEAS)**. The Joint communication for a European cyber defence policy mentions the establishment of an EU Cyber Skills Academy to develop skills to which the ECCC would have a key role as part of its missions to foster and encourage the development of cybersecurity competencies. Also, the joint communication deals with the EU level cyber reserve which could be part of the upcoming 2023 Cyber Solidarity Initiative. In anticipation, the ECCC could invest in DEP and HE projects that would boost the cybersecurity maturity of the EU industrial base. Then, it would provide grounds to build a European trusted ecosystem based on certification schemes for the cybersecurity industry.

There is a need to seek alignment with actions of the **European Defence Fund (EDF)** to avoid double spending.

Drafting the Agenda

In order to establish a coherent and inclusive Agenda, the process to develop this document followed the principles of consensus building. This process involved a good-faith effort to meet the interests of all stakeholders and to seek a unanimous agreement.

The process started in February 2022, with a workshop involving representatives of the NCCs and the ECCC. The workshop focused on the definition of the Agenda setting the ECCC strategic orientations, notably in view of future funding work programmes. In order to solicit ideas and input from the ECCC Governing Board (GB) and the NCCs, a discussion paper was developed as a first basis for the discussion on the Agenda. This document took inspiration from ‘The way forward’ report from February 2022, which was developed based on consultations with the four pilot projects and ECSO, in collaboration with ENISA and coordinated by DG CONNECT of the European Commission. In addition to receiving feedback from individual Member States, the European Commission also invited Member States to work together and submit multi-Member State contributions as appropriate.

The process continued with several meetings and workshops throughout 2022, both at a ECCC GB and NCC working group level, involving representatives of the Member States and the European Commission, as well as experts. In between these meetings, the representatives of the NCCs were asked to provide written input, which was gathered and processed by the co-chairs, and then shared again with the rest of the working group and the ECCC GB members to be discussed and finetuned in the subsequent session. This process resulted eventually in the final version of the Strategic Agenda as presented in this document.

The benefits of such a process included the creation of an engaged and empowered group of representatives of Member States, which will benefit from the future cooperation among the Network of NCCs and the ECCC. Additionally, the Network of NCCs developed a shared understanding to avoid challenges in the mutual cooperation.

[13] https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1662

[14] File at: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf and more context info here: https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/

[15] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6642

To ensure the Agenda continues to reflect the strategic innovation topics of the EU member states, the ECCC GB will be responsible for providing a review mechanism to ensure an agile adaptation to systemic changes impacting the cybersecurity environment. In addition, it is important to support the identification of future research and development challenges together with relevant stakeholders (academia, cybersecurity industry and SMEs, public authorities) and adjust the ECCC's strategic focus accordingly.

Key Impact Areas of the Strategic Agenda

The Agenda sets out a process to achieve the mission of the ECCC and the Network of NCCs through a series of strategic measures. Achieving the three mission statements laid out in the Regulation would benefit from more specific, measurable, achievable, relevant and time-specific impact statements which describe a desired outcome. These impact statements have been developed and form the framework for the Agenda. They stem from the core mission as set out in the Regulation for the ECCC and the Network, namely to:

a) strengthen its leadership and strategic autonomy in the area of cybersecurity by retaining and developing the Union's research, academic, societal, technological and industrial cybersecurity capacities and capabilities necessary to enhance trust and security, including the confidentiality, integrity and accessibility of data, in the Digital Single Market;
b) support the Union's technological capacities, capabilities and skills in relation to the resilience and reliability of the infrastructure of network and information systems, including critical infrastructure and commonly used hardware and software in the Union; and
c) increase the global competitiveness of the Union's cybersecurity industry with a strong focus on SMEs and startups, ensure high cybersecurity standards throughout the Union and turn cybersecurity into a competitive advantage for other Union industries.

To achieve this mission, the Strategic Agenda sets three short-term impact statements (2023-2027).

1. **By 2027, the ECCC and the Network will have funded European SMEs in developing and using strategic cybersecurity technologies, services and processes through a coordinated cascade funding mechanism via NCCs and national co-financing that lowers the application threshold for SMEs.**

Supporting EU SMEs delivers on the mission of the ECCC and the Network so that by 2027, the ECCC will have invested in projects that will level up the cybersecurity maturity of the European industrial base and workforce. It will enable the EU to increase its capacity to anticipate, face and respond to cyber incidents by relying on a European trusted community.

Furthermore, SMEs play a crucial role in the cybersecurity ecosystem by providing capability and capacity to local, regional and national stakeholders who will be using their tools and services to secure their data and network and information systems. Many SMEs also play a crucial role as providers of essential societal services or as critical links in digital supply chains and may be vulnerable to cybersecurity incidents potentially causing severe societal impact. The Agenda urges to always consider ways in which SMEs can make use of EU funding by offering national (NCC-led) funding as well as direct funding under the DEP and HE.

NCCs play a crucial role in lowering the threshold in applying for funding by providing not only direct funding, but also support and expertise to cybersecurity-focused SMEs in finding relevant funding for their innovation initiatives and linking relevant parties to each other through an active network of stakeholders.

Increasing the number of SMEs who participate in the projects set out by the action plan will result in an increased number of competitive tech/projects/initiatives resulting from ECCC action, leading to increased digital resilience, enhanced industrial capabilities as well as leadership of Europe.

2. **By 2027, the ECCC and the Network will have supported and grown the cybersecurity professional workforce in both quantity and quality through the standardisation and certification of cybersecurity skills and investments in education and training of cybersecurity professionals.**

Securing a skilled cybersecurity workforce is a crucial need for the Member States to achieve the mission of the ECCC and the Network, to enact the priorities set out in this Agenda and to deliver results of the action plan and other relevant European policy decisions. The Agenda addresses the need to increase the number of cybersecurity professionals by encouraging the promotion of the cybersecurity profession and to increase accessibility to innovative and state of the art educations and trainings for cybersecurity professionals. The cybersecurity workforce needs to include cybersecurity professionals not only with pure technical backgrounds, but also with other professional backgrounds, such as legal, psychological/behavioural, pedagogic and business administration backgrounds.

The projects stemming from this Strategic Agenda and action plan should facilitate communication between educators and employers to identify cybersecurity skills needed to support the mission of the ECCC and the Network. The Strategic Agenda and the specific actions should support standardisation and certification of cybersecurity skills (such as an open, accessible and inclusive European Cybersecurity Skills Framework) to support the needs of the employees and employers in the cybersecurity field.

3. **By 2027, the ECCC and the Network will have strengthened the research, development and innovation expertise and competitiveness of the EU cybersecurity community through the development and implementation of an efficient and coherent action plan.**

Guided by this Agenda, the action plan should address and steer investments by the joint European funds (specifically, but not exclusively, the cybersecurity work programs of the DEP and HE) in a comprehensive and strategic way, determining the best possible roadmap for addressing joint European cybersecurity challenges and the mission of the ECCC and the Network.

The action plan will take into account trends in technology at national level and EU policy developments to support the capacities, capabilities and skills needed to ensure high level of cybersecurity competence when addressing the resilience and reliability of the infrastructure of network and information systems.

The action plan will be designed to be as specific as needed but as flexible as possible in order to be able to react to market, technology and policy developments.

Priorities and actions

To achieve the vision of this Agenda, it is necessary to set priorities and actions that are deemed of strategic importance in boosting cybersecurity innovation in Europe. Thus, the priorities and actions listed in the Agenda have been weighed against and viewed through the lens of the three impact statements: do they contribute to achieving the mission? Please note that the actions presented below do not reflect any order of priority.

1. The following actions are prioritised to support SMEs to develop and use strategic cybersecurity technologies, services and processes:

1.1 Processes and tools for managing cybersecurity information and risk management

1.1.1 Develop and implement technologies, services and processes for supporting information sharing, coordinated and collaborative prevention, detection and response/recovery and investigation of cybersecurity incidents. This includes the development and deployment of Security Operations Centres (SOCs) across sectors and value chains, as well as strengthening the capacities and resources of the national reference CSIRT/CERT in essential and important entities defined in NIS2 and other related directives or legislations. It also includes the support and enhancement of CSIRT/CERT communities and Information Sharing & Analysis Centres (ISACs), supporting timely and secure cross-border exchange of notification data or single entry points for incident/breach notification (including mitigation actions for response and supporting cyber investigations).

1.1.2 Support awareness raising and subsequent adoption in organisational vulnerability management and development of Coordinated Vulnerability Disclosure (CVD) initiatives looking to remediate vulnerabilities, in alignment with ENISA. To create the conditions for a wider acceptance of CVD, emphasis will be on the use of CVD in public bodies promoting eGovernment services and the development and implementation of mechanisms to timely share relevant information with the software and hardware suppliers and software development community.

1.1.3 Develop and implement innovative modelling and simulation solutions for network security optimisation and optimisation of response options against current and emerging cyber threats. Examples are the development of digital twins (a digital representation of an intended or actual real-world cybersecurity product, system, or process), or modelling and simulation of current and future capabilities of potentially hostile actors in order to develop better solutions.

1.1.4 Ensure the availability of easily accessible and user-friendly cybersecurity tools for SMEs. This includes the development of products and tools developed from a human-centred design perspective (reducing the human factor risk), AI-based technologies for anomaly detection and assisting decision-making, cybersecurity maturity self-assessment tools and availability of risk modelling solutions from EU providers, including tools and frameworks aimed at SMEs to conduct a pragmatic Business Impact Analysis, Risk Analysis or Threat Model Analysis. In addition, SMEs should also (legally and practically) receive and benefit from Cyber Threat Intelligence (CTI), Indicators of Compromise, Threat Advisories, and translate complex CTI into more understandable language to make it actionable for SMEs.

1.2 Secure and resilient hardware and software systems

1.2.1 Increase the resilience of essential and important entities defined in NIS2 including their digital supply chain against cyber threats, in line with the CRA and NIS2 directive. Specific attention goes to emerging technologies identified in The EU's Cybersecurity Strategy for the Digital Decade (i.e. cloud, 5G, IoT, blockchain), as well as underlying infrastructure resilience of secure European DNS servers with embedded security and privacy, support to European trust service providers supplying certificates and the manufacturing and adoption of secure Galileo PRS time and position signal receiving infrastructure.

1.2.2 **Support the development and adoption of automation tools for cybersecurity processes by developing and deploying AI-based cybersecurity solutions** in line with the AI Act and ensure the security of AI-based solutions from adversarial AI threats/attacks. This development influences the activities of the cybersecurity professionals using these tools, and therefore links to the actions mentioned under 3.2. It is also important to consider how to make these automated solutions accessible to SMEs with limited to no cybersecurity expertise, in order to enable them to implement relevant actions.

1.2.3 **Promote security and privacy 'by design'** in emerging technologies, applications and hardware, including IoT, e-Identity and e-government systems, by supporting and/or funding research & development opportunities. This should increase the security of widely used technologies and promote the use of secure solutions and technologies, such as Privacy Enhancing Technologies. This action should stimulate organisations to increase the cyber resilience of their infrastructure, products and services and adhere to the Cyber Resilience Act and Network and NIS2 Directive.

1.2.4 **Support for implementing cybersecurity solutions in product development and prolonged use in (both old and new) IT/OT environments** such as automotive, energy production and water management, and seek convergence between safety and cybersecurity.

1.2.5 **Support the development, implementation and assurance (use of audits) of post-quantum cryptography in secure products and services**, including side-channel resistance of the implementation as well as the agility to switch between different cryptographic solutions when appropriate.

2. The following actions are prioritised to support and grow the professional workforce:

2.1 Development of cybersecurity skills: education and professional training

2.1.1 **Ensure the development, adjustment and adoption of educational curricula aligned with the needs of the market**, the public sector, as well as fostering entrepreneurship skills and international exposure. This includes the practical adoption of qualification and competence frameworks and similar tools to support academia in the development or adjustment of cybersecurity curricula and the facilitation of student exchanges amongst European universities (ERASMUS program) based on expertise and competences and between academia and EU organisational practice. Thus, better cooperation between theory and practice is stimulated, academia are in a position to excel in their specific expertise and a 'brain drain' in the EU can be better prevented.

2.1.2 **Develop common tools and easily accessible platforms for hands-on technical education, training and testing opportunities** in the area of cybersecurity including fighting cybercrime. Develop innovative training approaches for example through "gamification" and support of extracurricular activities for cybersecurity professionals in the cyber domain (e.g. cyber volunteers, reservists), including relevant initiatives within the European Commission's Cybersecurity Skills Academy.

2.1.3 **Deploy dedicated campaigns for cybersecurity career path development** to stimulate young professionals and students of all ages and genders to pursue and advance in cybersecurity careers. This includes the promotion of diversity and equality in professions in the cyber domain, also by supporting specific initiatives for attracting more women and girls in this career path. It also includes the development of (1 to 2-year) cross-career cybersecurity education programmes for professionals with non-cybersecurity occupations (lawyers, psychologists, teachers, business administration professionals etc).

2.1.4 **Promote security and privacy 'by design' approach in training and education** for IT professionals and developers to increase awareness and competencies on integrating security and privacy in (future) development of products and services, especially for start-ups and in software programming-related curricula.

2.1.5 **Promote the development of capabilities for cyber professionals on pre-threat management and prevention.** This action includes the foresight and forecasting analysis of cybersecurity trends, the early identification of threats, even if they have not yet become incidents; the identification and monitoring of the actors behind the threats, as well as their evolution and capabilities; the protection of society from identified novel threats; and the provision to law enforcement authorities with the tools they require for a more effective fight against threat actors. It is more efficient to identify and stop a threat before it causes significant damage.

2.1.6 **Increase awareness of cybersecurity threats, threat actor modi operandi and potential impact**, especially for vulnerable organisations such as SMEs, smaller public authorities, as well as vulnerable groups in society and children in primary and secondary education. This includes awareness campaigns and the promotion of actionable good practices by supporting the development and dissemination of dedicated training material and embedded training in daily life situations and supports the risk reduction posed by the human factor.

2.2 Cybersecurity skills framework and competence assessment

2.2.1 **Ensure the adoption and implementation of cybersecurity skills frameworks** as a lexicon to align cybersecurity related educational curricula with market needs, including the European Cybersecurity Skills Framework (ECSF).

2.2.2 **Support the development and dissemination of competence assessment and certification schemes** for personnel working in the cyber domain, to increase assurance of personnel quality and to improve expertise.

3. The following actions are prioritised to strengthen research, development and innovation expertise in the broader European cybersecurity ecosystem:

3.1 Promoting post-quantum cryptography standardisation and adoption

3.1.1 **Support expert organisations and post-quantum cryptography professionals to lead the development of adequate and robust post-quantum cryptography algorithms** by facilitating ongoing dialogue and consensus between different parties. Post-quantum cryptography standardisation also contributes to the interoperability of hardware and software.

3.1.2 **Develop Post-Quantum Cryptography adoption strategy with priorities based on risk analyses** (for both public and private organisations), taking into account appropriate migration paths, hybridisation, crypto-agility, and ensure that crypto-agility permits the timely implementation of mitigation plans for securing existing data. This can be fostered by strengthening post-quantum cryptography research & innovation, and secure deployment activities.

3.2 Support for European Cybersecurity Certification

3.2.1 **Encourage and facilitate industry uptake, encompassing SMEs, of mature European cybersecurity certification schemes and conformity assessments of essential requirements for cybersecurity products and services**, in order to support the development of a strong European industrial base. This includes supporting the European cybersecurity community and national cybersecurity certification authorities, and notifying and supervisory authorities to develop awareness, capacity, skills and expertise to facilitate the implementation of the European Cybersecurity Certification Frameworks (aligned with ENISA) and the Cyber Resilience Act. This ensures the recognition across Member States with the dissemination and uptake of efficient cybersecurity schemes of ICT products, processes and services/products with digital elements.

3.2.2 **Enhance pan-European conformity assessment systems** in support of harmonisation, cooperation and re-use (e.g. the development of a platform to assist conformity assessment bodies, proficiency testing schemes and standardisation) and supporting the development and dissemination of tools for the benefit of conformity assessment efficiency (e.g. code analysis and vulnerability assessment tools).

3.3 Strengthening market competitiveness

3.3.1 **Develop an understanding of the cybersecurity community by dynamically mapping its capacities and capabilities and identification of potential collaboration opportunities**. This improves the adoption of national observatories on accessibility of EU cybersecurity financial support and on subsequent analysis of the implications arising for a secure, robust and continuous Digital Single Market.

3.3.2 **Support the uptake of EU cybersecurity technologies and products**, by developing a strategy (and support its implementation) to support the European cybersecurity start-up/SME ecosystem, in collaboration and complementarity with the European Innovation Council and ongoing national and regional initiatives, such as accelerator and incubation programmes and technology transfer programmes. Such a strategy should also include support for scale-ups, taking into account the use of public procurement and private investment direction.

3.3.3 **Support an EU-wide open cybersecurity marketplace** in which smaller players can sell immediately at EU scale and to larger organisations, and in particular where certification is not used to protect national markets. This action increases visibility of EU cybersecurity products and services on a global level.

3.4 Promoting collaboration and information sharing

3.4.1 **Encourage collaboration amongst institutions for higher education, interdisciplinary research and innovation**, as well as between these institutions and industry in order to apply innovation in practice. Examples of this are the exchange of personnel, scientist-on-the-job, summer schools, interdisciplinary educations, and the development of cyber campuses.

3.4.2 **Promote the creation and capacity building of Information Sharing and Analysis Centre (ISAC) style cooperation initiatives** in cross-border, cross-sectoral, cross-community (including with law enforcement and cyber defence) and multi-lingual contexts, using standardised taxonomies and/or ontologies and comparable maturity indicators. The increase of shared cybersecurity information is beneficial on multiple layers: it supports improved security measures from sharing experiences and lessons learned, research activities, organisational risk management decision-making, detection and incident response, as well as other relevant domains.

3.4.3 **Encourage collaboration to enhance cyber resilience** between authorities, supplementing under Directive (EU) 2022/2555 and without prejudice to its structures, in particular the NIS Cooperation Group, to raise cybersecurity maturity levels through development and implementation of common methodologies for peer assessment and learning, through exchange of personnel and through joint projects to aid mutual understanding and assistance. This should enable deployment of cybersecurity processes and the uptake of products and services by essential and important entities under section 2.2.1.