ECCC

EUROPEAN CYBERSECURITY COMPETENCE CENTRE

ECCC Digital Europe Program 2025-2027

Cybersecurity & Trust

Draft V4, clean

Version 4 following November GB Meeting

December 2024

[To be added copy right notice, legal notice, contact info.]

Table of Contents

Table of Contents 3
1 Introduction 5
1.1 Policy Context 7
1.2 DEP overall objectives 10
1.3 Specific objectives 10
1.4 Indicative budget allocation 11
1.5 Other considerations 12
1.6 Calls structure and planning 15
2 Deployment actions in the area of cybersecurity 17
New technologies. AI & transition to post quantum 17
2.1 Cybersecure tools, technologies and services relying on AI 17
2.2 Strengthening cybersecurity capacities of European SMEs with cybersecure AI powered solutions 20
2.3 Deployment of a European testing infrastructure for the transition to PQC in different usage domains 24
2.4 Transition to post-quantum Public Key Infrastructures 26
2.5 Migration of Cyber-hubs to PQC 29
2.6 Uptake of innovative cybersecurity solutions for SMEs 31
Cyber Solidarity Act Implementation 34
2.7 National Cyber Hubs 36
2.8 Cross-Border Cyber Hubs 40
2.9 Strengthening the Cyber Hubs ecosystem and enhancing information sharing 44
2.10 Coordinated preparedness testing and other preparedness actions 46
2.11 Mutual assistance 49
Additional actions for improving EU cyber resilience 51
2.12 Enhancing the NCC network 51
2.13 Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements 56
2.14 Dedicated action to reinforcing hospitals and healthcare providers 62
2.15 Dual use technologies 64

3 Programme Support Actions 67
4 Implementation 67
4.1 Procurement 68
4.2 Grants – Calls for Proposals 68
5 Appendices 70
Appendix 1 – Award Criteria for the Calls for Proposals 70
Appendix 2 – Types of action to be implemented through grants 70
Appendix 3 - Implementation of Article 12(5) Regulation (EU) 2021/694 72
Appendix 4: Restrictions for the protection of European digital infrastructures, communication and information systems, and related supply chains 73
Appendix 5 - Abbreviations and Acronyms 75

1 Introduction

In a changing geopolitical context, the EU strives to strengthen its leadership and strategic autonomy in the area of cybersecurity. To achieve it, in December 2020, the Commission and the High Representative presented the EU's Cybersecurity Strategy for the Digital Decade[1], which inter alia sets out the objective to develop the EU's technological sovereignty in cybersecurity, building capacity to secure sensitive infrastructures such as 5G, and reduce dependence on other parts of the globe for the most crucial technologies. The Strategy also acknowledges that EU policies and investment in cybersecurity are a cornerstone of the EU Security Union Strategy[2]. The efforts needed to achieve the aforementioned goals are not limited to Research and Development; The *Digital Europe Programme*[3], with *Specific Objective 3: Cybersecurity and Trust* is designed to co-invest on deploying research and development solutions from cybersecurity domain, to have a multiplication effect on the research results.

A pillar of the EU cybersecurity strategy is the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) with the Network of National Coordination Centres (NCCs)[4]. The ECCC is Europe's initiative to support innovation, industrial policy and research in cybersecurity. The Centre develops and implements, with Member States and countries associated to Specific Objective 3 of the Digital Europe Programme, industry and the academic Community, a common strategic agenda[5] for cybersecurity technology development and deployment in strategic areas for the benefit of SMEs and public administration. The Network of National Coordination Centres and the Centre together will enhance our technological sovereignty by supporting projects in critical areas.

The Digital Europe Programme (DEP) supports the co-investment strategy foreseen by EU regulation 2021/887 establishing the ECCC. For the Specific Objective 3 dedicated to Cybersecurity, until 2023, the Work Programme (WP) on Cybersecurity of the Digital Europe Programme were developed under the leadership of the European Commission for 2021-2022[6], for 2023-2024 and the amendment of the latest[7]. With DEP, which is dedicated to

[1] Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade (JOIN(2020)18)
[2] Communication to the European Parliament and the Council on the EU Security Union Strategy (COM/2020/605 final)
[3] DEP Regulation (EU) 2021/694
[4] Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research.
[5] The ECCC Strategic Agenda available at: https://cybersecurity-centre.europa.eu/strategic-agenda_en
[6] To add link to 2021-2022
[7] Amended DEP WP for cybersecurity for 2023-2024, available at: https://ec.europa.eu/newsroom/dae/redirection/document/100739

deployment of the cybersecurity solutions, it is foreseen to ensure uptake of research results delivered by the Horizon Europe programme, dedicated to finance European research.

The application of Article 12(5) of the Digital Europe Programme Regulation limits[8] the participation to entities established in and controlled from eligible countries (Appendix 3)[9]. The Cyber Solidarity Act, as resulted from the political agreement between the co-legislators, provide for amendments to Articles 12(5) and (6) of the Digital Europe Programme Regulation allowing for flexibility beyond of the application of Article 12(5) (i.e. to purchase from non-EU controlled companies). This will be based on a biennial (at least every two years) mapping by European Cybersecurity Competence Centre (ECCC) of tools infrastructure and services needed by Cyber Hubs, including their availability from EU established and EU controlled entities[10]. The first mapping exercise will start in late 2024 in consultation with the CSIRTs network, the existing Cross-border Cyber Hubs, ENISA and the Commission.

With this Work Programme (WP), foreseen for interval 2025-2027, the aim is to cover the remaining actions and budget foreseen in DEP Regulation (EU) 2021/694 dedicated to the *Specific Objective 3: Cybersecurity and Trust* and at the same time are implemented by ECCC. This Cybersecurity WP is meant to complement the Main DEP WP.

This is the first DEP Work Programme developed by ECCC in close consultation with its Governing Board (GB) and with the European Commission. This document includes inputs from the strategic documents[11] as prepared by the GB and NCCs, and takes into account all the legal obligations stemming from the ECCC regulation, the DEP regulation, the Cyber Solidarity act, while supporting the implementation of the Cyber Resilience Act, the Cybersecurity Act, NIS 2 Directive, etc.

[8] This limitation could be waved, as per Cyber Solidarity Act, following the outcome of a future ECCC mapping of infrastructures, tools and services offered, including from EU controlled and non-EU controlled companies. If there is not enough from EU controlled and the security risks does not outweighs this lack of offer, Article 12(6) of DEP Regulation can be used - see additional document with explanations. This means that the ECCC would need to conduct mapping before the WP is adopted to be able to decide. If art 12(6) will be used for Cyber Hubs, this sentence would need to be changed.

[9] Calls for proposals and calls for tenders funded under this WP will be restricted to legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States. European Economic Area-European Free Trade Association (EEA EFTA) countries are fully associated to the Digital Europe Programme and benefit from a status equivalent to that of the Member States. (Appendix 3).
EEA EFTA countries are fully associated to the Digital Europe Programme and benefit from a status equivalent to that of the Member States.

[10] The decision to apply Article 12(5) or 12(6) of DEP will be done in the DEP work programme and will concern the work programmes after the adoption of the Cyber Solidarity Act, so the current work programme 2025-2027 is also impacted. The mapping exercise foreseen in Cyber solidarity Act did not start and needs to be delivered to be able to have this decision taken.

[11] The ECCC Strategic Agenda was published in March 2023. It is available here: https://cybersecurity-centre.europa.eu/strategic-agenda_en

About this document

The document is the result of several rounds of consultations involving the ECCC governing board. Following the initial discussion, that took place during the June 2024 Governing Board (GB) meeting, the GB members provided written comments until July. The feedback received was taken into account in preparation of a consolidated version circulated in September. A second round of consultation took place in October and during October GB meeting. Last consultation took place in November, including an Ad-Hoc Governing Board meeting organized on 20 November. The current version takes in consideration the most recent feedback of European Commission and the priorities that President-elect Von Der Leyen presented in her Political Guidelines 2024-2029 in front of the European Parliament Plenary on 18th July 2024[12].

This updated version focuses on the actions foreseen for 2025, to facilitate an agreement on the actions to be delivered and the budget to be implemented in 2025, to allow adoption of ECCC Single Programming Document (SPD) 2025-2027.

The goal is to have a consolidated and comprehensive DEP WP before final approval.

- *The topics indicated in the WP have been selected using the following guiding documents:*
  - *The ECCC regulation and ECCC objectives*
  - *the 2023 Strategic Agenda and other documents*
  - *the tasks list foreseen in the Cyber Solidarity Act[13], which specifies activities to be financed or delivered by ECCC[14];*
  - *Other regulations or directives, already in force or to enter into force requiring specific cybersecurity measures across EU, like NIS 2 directive, Cybersecurity Act, Cyber Resilience Act, GDPR, DORA, etc.*

1.1 Policy Context

The preparation of the Cybersecurity DEP Work Programme 2025-2027 is taking place in a dynamic cybersecurity political context, including several initiatives at EU level:

- **Revision of the NIS Directive (NIS2).** To respond to the increased exposure of Europe to cyber threats, the EC proposed, in December 2020, a revision of the NIS Directive (NIS 2 Directive). The Directive was adopted in December 2022, and the national transposition measures shall be applied as from 18 October 2024. The new Directive raises the EU common level of ambition on cyber-security, through a wider scope, clearer rules and stronger supervision tools.
- **Cybersecurity Resilience Act (CRA).** In September 2022, the EC presented the proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act, CRA)[15]. The CRA establishes a horizontal legal framework for cybersecurity essential

[12] Link: https://commission.europa.eu/about-european-commission/president-elect-ursula-von-der-leyen_en
[13] Still to be published, however ECCC work needs to be aligned asap with the provisions from the Regulation.
[14] 7589/24 ADD 1 from 18/03/2024
[15] Proposal for Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM/2022/454 final.

requirements for placing products with digital elements on the market. The CRA aims to ensure that hardware and software products are placed on the EU market with fewer vulnerabilities and that manufacturers take cybersecurity seriously throughout the whole product lifecycle. It also aims to create conditions that allow users to take cybersecurity into account when selecting and using products with digital elements. On 30 November 2023, the co-legislators have agreed on a political compromise text for the legislative proposal and the Cyber Resilience Act is expected to enter into force in the course of 2024.

- **Cyber Solidarity Act.** In April 2023, the Commission adopted a proposal for a Cyber Solidarity Act, including amendments to Digital Europe Programme Regulation, designed to: (1) strengthen common coordinated Union detection capacities and common situational awareness of cyber threats and incidents; (2) reinforce preparedness and enhance response and recovery capacities to handle significant, large-scale and large-scale equivalent cybersecurity incidents; (3) enhance union resilience and contribute to effective response by reviewing and assessing significant or large-scale incidents. The Cyber Solidarity Act will complement ECCC actions to provide long-term solutions to strengthen solidarity at Union level. On 6 March 2024, the co-legislators have agreed on a political compromise text for the legislative proposal and the Cyber Solidarity Act is expected to enter into force in the course of 2024. The Cyber Solidarity Act provides for a number of actions for the ECCC to implement. The ECCC will be responsible for actions related to the European Cybersecurity Alert System, including managing the joint procurement with Member States of tools, infrastructures and services needed for the Cyber Hubs, the accompanying grants and conducting the mapping of the tools, infrastructures and services necessary to establish or enhance National Cyber Hubs and Cross-Border Cyber Hubs. The ECCC will also be responsible under the Cybersecurity Emergency Mechanism for managing the calls for grants for the preparedness actions, including coordinated preparedness testing and other preparedness actions and managing the support within the mutual assistance action.
- **Measures for a high common level of cybersecurity for EU institutions, bodies, offices and agencies.** The EC presented a proposal for a regulation to enhance the cybersecurity and information security of the EU institutions, bodies, offices and agencies, which entered into force in December 2023. Regulation 2023/2841 puts in place a framework for governance, risk management and control across EU entities in cybersecurity, with new competences and attributions for CERT-EU and a new interinstitutional Cybersecurity Board to monitor the Regulation's implementation.
- **European Cybersecurity certification schemes**. The European Cybersecurity Certification Framework laid out in the Cybersecurity Act[16] aims at creating market-driven European cybersecurity certification schemes and increasing "cybersecurity-by-design" in ICT products, services, and processes. On 5 March 2024, the co-legislators have agreed on a political compromise text for an amendment of the Cybersecurity Act enabling the future adoption of European certification schemes for managed security services. This amendment is expected to enter into force in the course of 2024. The first European Cybersecurity Certification scheme, the Common Criteria-based European cybersecurity certification scheme (EUCC) has been adopted, and two

[16] Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

other schemes are currently being prepared, based on preparatory work coordinated by ENISA: the European Cybersecurity Certification Scheme for Cloud Services (EUCS) and the European 5G Certification Scheme (EU5G). In support of certification, the EU Standardisation Strategy and the current EU funding framework both include essential topics such as the development of harmonised evaluation methodologies or promoting innovations to the performance of testing ICT products, services and processes.

- **EU 5G Toolbox.** The EU 5G Toolbox[17] is a comprehensive and objective risk-based approach for the security of 5G and future generations of networks. In June 2023, the NIS Cooperation Group adopted a report on the status of implementation of the EU 5G Toolbox[18], which showed that a vast majority of Member States have reinforced or are in the process of reinforcing security requirements for 5G networks based on the EU Toolbox, but some of the key measures have not been fully implemented yet in all Member States. The EC also adopted a Communication on this topic at the same time[19], in which it underlined its strong concerns about the risks to EU security posed by certain 5G suppliers and committed to ensure that its own corporate communications and Union funding activities will not rely on these suppliers. In addition, the NIS Cooperation Group, with the support of the EC and ENISA, carried out a risk assessment on the telecommunications sector[20] at large and identified a number of key threats that could pose significant risks for the security and resilience of the connectivity infrastructure. To mitigate these risks, a number of strategic and technical recommendations for Member States, the Commission and ENISA, are put forward.
- **EU funding in the 2021-2027 Multiannual Financial Framework.** In 2022 and 2023 funding was provided for projects on cybersecurity deployment under the DEP, and for cybersecurity research under the HEP, while further funding is foreseen under both EU programs. The respective work programmes 2023-2024, including support for cybersecurity, were adopted in 2023.
- **EU Cybersecurity Skills Academy.** In 2023 the EC adopted a non-legislative initiative outlining policy and support measures to promote cyber skills.
- **EU Cyber Defence Policy**. It was endorsed by Council Conclusions in 2023[21] and it includes references to the ECCC as an essential pillar to support the scale up of European cybersecurity industry.

[17] 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.

[18] NIS Cooperation Group, Second report on Member States' Progress in implementing the EU Toolbox on 5G Cybersecurity, 15 June 2023, https://digital-strategy.ec.europa.eu/en/library/second-report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity

[19] European Commission, Implementation of the 5G cybersecurity Toolbox, C(2023)4049 final, 15 June 2023.

[20] NIS Cooperation Group, Cybersecurity and resiliency of Europe's communications infrastructures and networks, 21 February 2024, https://digital-strategy.ec.europa.eu/en/library/report-cybersecurity-and-resiliency-eu-communications-infrastructures-and-networks

[21] The Council Conclusions on the EU Policy on Cyber Defence, as approved by the Council at its meeting held on 22 May 2023, available at: https://www.consilium.europa.eu/media/64526/st09618-en23.pdf

1.2 DEP overall objectives

The Digital Europe Programme will reinforce the EU's critical digital capacities by focusing on the key areas of artificial intelligence (AI), cybersecurity, advanced computing, data infrastructure, the deployment of these technologies and their best use for sectors such as energy, climate change and environment, manufacturing, mobility, agriculture and health.

The Digital Europe Programme also targets upskilling to provide a workforce for these advanced digital technologies. It supports industry, small and medium-sized enterprises (SMEs), and public administration in their digital transformation with a reinforced network of European Digital Innovation Hubs (EDIH).

1.3 Specific objectives

Actions in this work programme will in particular:

- Support the uptake of **new technologies for cybersecurity** and securing their implementations. As such, will facilitate the deployment of **Artificial Intelligence and cybersecurity**: financing the take-up of AI, including generative AI, cybersecurity of AI and AI for cybersecurity, tools and other key digital technologies for Cyber applications, as well as for improving and expanding the Cyber Hubs capabilities, while also contributing to strengthening European cyber resilience. It will also contribute to the **transition to the post quantum**; support for the transition to adopt Post Quantum Encryption technologies for industry and public administrations.
- **Deliver on the Cyber Solidarity Act**, by Contributing to the consolidation of **European Cybersecurity Alert System**: supporting the deployment of Cyber Hubs and Cross-Border Cyber Hubs in line with the recently agreed Cyber Solidarity Act, to support detection and build enhanced awareness regarding cybersecurity threats. It will implement the **Cybersecurity Emergency Mechanism** and support **preparedness actions** of Member States, in the context of the Cyber Solidarity Act, such as coordinated preparedness testing of entities operating in sectors of high criticality and other preparedness actions for entities operating in sectors of high criticality and other critical sectors. It will also support **mutual assistance** between Member States, in the context of the Cyber Solidarity Act.
- Support **additional policy implementation activities improving EU resilience**, including the implementation of NIS2 and the Cyber Security Act as well as the Cyber Resilience Act, while providing SMEs the tools to comply with regulatory requirements. Support the industry, SMEs and start-ups to comply with regulatory requirements, especially the NIS2[22] implementation or requirements concerning the

[22] See https://eur-lex.europa.eu/eli/dir/2022/2555

proposed Cyber Resilience Act[23]. A special focus will be on the **health sector**, to support the cybersecurity of hospitals and healthcare providers, in line with the priorities that President-elect Von Der Leyen presented in her Political Guidelines 2024-2029 in front of the European Parliament Plenary on 18th July 2024[24].

The Cybersecurity strategy identifies, scope for EU action in the area of "*resilience, technological sovereignty and leadership*" of the Union. It recognises that the EU's critical infrastructure and essential services are increasingly interdependent and digitised. All Internet-connected things in the EU, whether automated cars, industrial control systems or home appliances, the whole supply chains which make them available, as well as the underlying internet infrastructure need to be secure-by-design, resilient to cyber incidents, and quickly patched when vulnerabilities are discovered.

This Work Programme, prepared by ECCC[25], does not stand by itself in pursuing these objectives. Rather, it is complemented with actions in the Main Digital Europe WP implemented by European Commission or other EU bodies and agencies.

1.4 Indicative budget allocation

Digital Europe is implemented by means of multiannual Work Programmes. This Work Programme covers Cybersecurity topics that will be implemented by the ECCC.

The budget for Cybersecurity actions covered by this Work Programme is of EUR **353 million**, distributed across the 3 years 2025-2027. The **indicative** proposal for the distribution of budget across the whole period is as follows.

- EUR 127 million for **new technologies and cybersecurity**, the deployment of Artificial Intelligence & cybersecurity and the transition to the post quantum**.**
- EUR 111 million for the **implementation of Cyber Solidarity Act**, consolidation of **European Cybersecurity Alert System, Cybersecurity Emergency Mechanism/ preparedness actions** and **mutual assistance** actions of Member States.
- EUR 106 million for **additional actions improving EU resilience.**
- EUR 9 million for **programme support actions**, including evaluations and reviews.

The budget figures given in this WP are indicative and subject to change following GB discussion; Section 1.6 provides a tentative allocation for the interval 2015-2027.

---

[23] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0454

[24] Available at: https://commission.europa.eu/about-european-commission/president-elect-ursula-von-der-leyen_en ; One initiative announced in the Guidelines '*We must also do more to protect the security of our health systems, which are increasingly the target of cyber and ransomware attacks. To improve threat detection, preparedness and crisis response, I will propose a European action plan on the cybersecurity of hospitals and healthcare providers in the first 100 days of the mandate.*' has a direct impact on our work.

[25] Not all financing for *Specific Objective 3: Cybersecurity and Trust* is implemented by ECCC. This document only covers topics implemented by ECCC.

1.5 Other considerations

1.5.1 Third countries participation

Dependencies and vulnerabilities in cybersecurity can open the door to increased undue influence and control over key industrial assets as well as over providers of critical infrastructure and essential services. This in turn can lead to disadvantageous knowledge transfers and long-term economic costs and make Europe susceptible to undue foreign influence. Cybersecurity incidents can be either accidental or deliberate action of criminals, state and other non-state actors. Cybersecurity attacks on infrastructure, economic processes and democratic institutions, undermine international security and stability and the benefits that cyberspace brings for economic, social and political development.

Therefore, the security interests of the Union in the area of cybersecurity require building capacity to secure sensitive infrastructures through cybersecurity solutions and reducing excessive dependence on other parts of the globe for the most crucial technologies.

All actions under this WP aim at increasing the EU's collective resilience against cybersecurity threats. Furthermore, several actions in this Work Programme will establish tools, infrastructures and resources intended specifically for the use of cybersecurity authorities in Member States in defending against criminal and/or politically motivated cyber threats, including in particular supply-chain attacks.

In order to protect the essential security interests of the Union, the implementation of some of the cybersecurity topics under the Digital Europe Programme should depend on legal entities (e.g., providers) established or deemed to be established in Member States and controlled by Member States or by nationals of Member States.

Because of this criticality, participation to some of the calls funded under this WP may be, depending on the topic, subject to the provisions of Article 12(5) of the Digital Europe Programme Regulation, as indicated in each relevant topic. Those calls for proposals and calls for tenders for these topics shall be restricted to legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States. EEA EFTA countries are fully associated to the Digital Europe Programme and benefit from a status equivalent to that of the Member States. Further information is included in *Appendix 3 - Implementation of Article 12(5).*

Please note that further to conclusion/performance of the Mapping in accordance with the Cybersecurity Act, the WP text will be amended to reflect the results of the assessment and set the security conditions accordingly for national and Cross-Border Cyber Hubs.

1.5.2 Links to programmes and co-investments

Most actions foreseen in the Digital Europe Programme require co-investments from the public and private sectors. The modes of these co-investments are described in the relevant parts of the various work programmes.

As far as possible funding support from other EU instruments to actions in this WP is concerned, alternating or cumulative funding may be considered, provided that such funding is in line with the fund-specific regulations of the funding instruments in question, and in line with the objectives of the relevant programmes. Relevant provisions of the Financial Regulation need to be respected[26], in no circumstances the same costs shall be financed twice by the EU budget (prohibition of double funding). Funding from cohesion policy programmes can fall under EU State aid rules when the beneficiaries are undertakings. In such cases, the funding must be compatible with EU State aid rules.

An alternating/sequenced funding occurs when each instrument finances a different part of the operation/action, or finances successive parts. It requires a split of an operation/action in two different parts. Separate grant agreements are required, applying the rules of the funding instruments respectively. Coordination is required to avoid double funding, ensuring the separation of parts/activities. Expenditure used for a reimbursement request for one instrument shall not be declared for support from another Fund or Union instrument. Activities financed under separate instruments have to be clearly differentiated.

Cumulative funding means that an operation/project receives support from more than one fund, programme or instrument (including both shared and directly managed funds) for the same item of cost/expenditure. Two grant agreements are required, applying the rules of each of the funding instruments respectively. Upfront coordination is required to avoid double funding by coordinating the funding rates which in combination cannot go over 100% of the eligible costs. A number of steps starting from preparation, through linking of actions, grant signatures all the way to reporting and payments need to be followed. The Commission Notice on Synergies between Horizon Europe Programme and the European Regional Development Fund (ERDF) programmes[27] elaborates on new opportunities to maximise synergies between Horizon Europe and the ERDF, including on cumulative funding. An example on how such cumulative funding is applied to Digital Europe Programme and cohesion policy funds is outlined in the Appendix 2 of the Notice.

Member States shall ensure the effective and efficient functioning of such synergies, through a consistent and harmonised approach of all involved authorities and close coordination between all public actors is needed.

Funding from cohesion policy programmes and national budgets can fall under EU State aid rules when the beneficiaries are undertakings or supported activities are of an economic nature. In such cases, the funding must be compatible with EU State aid rules.

[26] In particular the Article (191) Principle of non-cumulative award and prohibition of double funding

[27] Synergies between Horizon Europe and the ERDF programmes (2022); https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/synergies-guidance-out-2022-07-06_en

Below is an outline of actions for which cumulative funding could be considered. However, support from multiple funding sources is in all cases subject to decisions of the authorities managing the funding instruments.

Table 1: Actions for which cumulative funding could be considered

Topics in the Work Programme	**DIGITAL Funding rate**
Cyber Hubs / cross border	75% for Joint Procurement and 50% for Grants
Cyber Hubs / others	50% procurement 50% for grants
AI, PQC, preparedness, others	50%

1.5.3 Multi Country projects and the European digital infrastructure consortia

As part of the Path to Digital Decade policy programme proposal[28], the Commission has introduced the concept of Multi-Country Projects (MCPs). MCPs are large-scale deployment and capacity-building projects for the digital transformation of the Union, facilitating the achievement of the Digital Decade objectives and targets[29]. They channel coordinated investments between the EU, Member States and private stakeholders to, i.e., enable digital infrastructure projects that one single Member State could not deploy on its own. They help reinforce the Union's technology excellence and industrial competitiveness in critical technologies, support an interconnected, interoperable and secure Digital Single Market and address strategic vulnerabilities and dependencies of the Union along the digital supply chain. This means that setting up a MCP in a relevant area fits the objectives of the Digital Europe Programme and provides additional incentives for Member States and companies to work together to build pan-European digital infrastructures.

A number of areas of MCP are in the scope of the Digital Europe Programme and are receiving funding under the Digital Europe Main WP 2021-2022, 2023-2024 and Cybersecurity WP.[30] The MCPs in this WP are dedicated to Cyber Hubs and is part of section 2.1.

EU State aid rules apply to the public funding granted from Member State resources if that funding is for an economic activity or benefits this activity, and if all other cumulative conditions for the presence of State aid, set out in Article 107 (1) TFEU, are met.

[28] Proposal for a Decision establishing the 2030 Policy Programme "Path to the Digital Decade" https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0574

[29] Digital Compass: the European way for the Digital Decade: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118

[30] The initial list of areas of activity for Multi-Country projects, as per Path to the Digital Decade Policy Programme Annex is listed in Annex 4 (Section 9.4) of the Main WP 2023-2024.

1.5.4 Climate and biodiversity

Digital tools have the potential to contribute to climate: AI can - via interconnected technologies - be an enabler for low-carbon smart cities and ensure that energy consumption is efficient, digital services remove the need for physical presence, data space can provide data to organisations that can help them improve the efficiency, energy consumption in specific sectors. Cybersecurity infrastructures and tools supported by this WP aim to support the use of such technologies by making them safe and thereby enabling their wider adoption. This ranges from consumer products to the protection of more efficient critical infrastructures and essential services, up to the capacity of organisations to detect cyber threats and to respond to attacks in an efficient manner and to ensure that authorities can be prepared for them. It will help Member States work together to be better prepared for large scale cyber-attacks. While cybersecurity is not aimed at, for instance, reducing the energy consumption of these tools, it is a precondition for using many technologies that do exactly this. As for biodiversity, cybersecurity does not directly contribute to the conservation and restoration of biodiversity (ecosystems, species, and genetic diversity), the maintenance of related ecosystem services; the sustainable use and management of biodiversity and ecosystems (including activities within agriculture, forestry, fisheries and other sectors); or the fair and equitable sharing of the benefits of the utilisation of genetic resources.

1.6 Calls structure and planning

This section lists all the proposed topics for 2025-2027. The topics are clustered around some big chapters, which are still very much connected. For instance, many of them are dedicated to implementation of EU legislation around cybersecurity. While some topics are dedicated to specific public entities - like the ones having the role of Cyber Hubs – many other topics are design to support SMEs.

A list of clusters is listed here:

- **New technologies and cybersecurity**: impact and benefits for cybersecurity of AI and post quantum transition.
- From Cyber Solidarity Act, **European Cybersecurity Alert System, Cybersecurity Emergency Mechanism and Mutual Assistance**.
- Implementation of EU legislation dedicated to **EU resilience**, including a topic targeting a sectorial priority and strengthening NCCs capabilities.

The following table provide an initial list of topics and chapters with an indicative budget per year. (values in million EUR).

Areas and topics with indicative allocations		2025	2026	2027	Total
New technologies. AI & transition to post quantum					**127**
2.1	Cybersecure tools, technologies and services relying on AI	15	15	15	45
2.2	Strengthening cybersecurity capacities of European SMEs with cybersecure AI powered solutions		20		20
2.3	Deployment of a European testing infrastructure for the transition to PQC in different usage domains	25			25
2.4	Transition to post-quantum Public Key Infrastructures	15			15
2.5	Migration of Cyber-hubs to PQC			7	7
2.6	Uptake of innovative cybersecurity solutions for SMEs	15			15
Cyber Solidarity Act Implementation					**111**
2.7	National Cyber Hubs	20	15		35
2.8	Cross-Border Cyber Hubs	20		20	40
2.9	Strengthening the Cyber Hubs ecosystem and enhancing information sharing		2		2
2.10	Coordinated preparedness testing and other preparedness actions	10	15	5	30
2.11	Mutual assistance		2	2	4
Additional actions improving EU cyber resilience					**106**
2.12	Enhancing the NCC network		35		35
2.13	Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements		20	11	31
2.14	Dedicated action to reinforcing hospitals and healthcare providers	30			30
2.15	Dual use technologies		10		10
Programme Support Actions		3	3	3	3
TOTAL		**153**	**137**	**63**	**353**

A tentative calendar is included here below for DEP 2025 calls. A similar timeline will be used for 2026 and 2027 calls.

	Digital Europe
Opening	Q1-Q2/2025
Closing	Q3-Q4/2025
Evaluation	Q1/2026
Signature of the grants	Q3/2026

2 Deployment actions in the area of cybersecurity

New technologies. AI & transition to post quantum

Under this section, several topics are presented. Some addresses the requirements of the public bodies and their needs for cybersecurity where AI could enable more efficient and effective solutions and also ensure a smooth transition to post quantum. Other topics are open for all types of beneficiaries aiming to strengthen their tools, products, solutions and infrastructures relying on cyber secure AI solutions or support transition to post quantum. Cybersecurity is the precondition for reliable, secure and resilient AI models and algorithms to be used and deployed under the following topics. Dedicated topics for SMEs are also included.

2.1 Cybersecure tools, technologies and services relying on AI

2.1.1 Objective

This topic addresses AI (including GenAI) based technologies for national authorities, including national and Cross Border Cyber Hubs, CSIRTs, competent authorities, public bodies and private entities from NIS 2 directive sectors, NCCs, etc. They play key role in providing central operational capacity to European cybersecurity ecosystems. They may also provide primary input data to ML. AI/ML based cybersecurity tools and solutions can strengthen such authorities' capacities to analyse, detect and prevent cyber threats and incidents, and to support the production of high-quality intelligence on cyber threats. In particular, the adoption of the generative AI[31] might be a challenge and an opportunity for cybersecurity[32] processes and applications.

These enabling technologies should allow more effective creation and analysis of Cyber Threat Intelligence (CTI), automation of large-scale processes, as well as faster and scalable processing of CTI and identification of patterns that allow for rapid detection and decision making.

The security of AI itself also needs to be addressed. This includes carrying risk assessment and mitigation of cybersecurity risks inherent in the AI technologies, implementing supply

[31] Cybersecurity in the age of generative AI, September 2023, available at: https://www.mckinsey.com/featured-insights/themes/cybersecurity-in-the-age-of-generative-ai

[32] The Need For AI-Powered Cybersecurity to Tackle AI-Driven Cyberattacks, April 2024, available at: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/the-need-for-ai-powered-cybersecurity-to-tackle-ai-driven-cyberattacks

chain security etc., and complying with the AI Act and requirements for intellectual property and the GDPR. The misuse of AI by malicious actors should not be ignored.

2.1.2 Scope

Actions in this topic should develop and deploy systems and tools for cybersecurity[33], based on AI technologies[34], addressing aspects such as threat detection, vulnerability detection, threat mitigation, incident recovery through self-healing, data analysis and data sharing. These activities must also comply with intellectual property rights (IPR) and the GDPR, depending on the type of information handled. The AI solutions proposed should also be cybersecure.

Activities should include at least one of the following:

- Continuous detection of patterns and identification of anomalies that can potentially indicate emerging threats, recognising new attack vectors and enabling advanced detection in an evolving threat landscape Including in ICT or in Operational Technology infrastructures using open technologies.
- Creation of CTI based on novel threat detection capabilities.
- Enhancing speed of incident response through real-time monitoring of networks to identify security incidents and generating alerts or triggering automated responses.
- Mitigating malware threats by analysing code behaviour, network traffic, and file characteristics, reducing the window of opportunity for attackers to exploit malware.
- Identification and support for management of vulnerabilities considering multiple sources of information.
- Support for recovery from incidents through self-healing capacities.
- Reducing the chances of attacks and pre-emptively identifying weaknesses through automated vulnerability scanning and penetration testing.
- Protecting business sensitive data through the analysis of access patterns and detection of abnormal behaviour.
- Enabling organisations to leverage and share CTI and other actionable information for analysis and insights without compromising data security and privacy, through anonymization.
- Tool and service providers are welcome to apply to this topic, also when in a consortium with Cyber Hubs. Links with stakeholders in the area of High-Performance Computing should be made where appropriate, as well as activities to foster networking with such stakeholders. In well justified case access requests to the EuroHPC high performance computing infrastructure could be granted.

[33] Multilayer Framework for Good Cybersecurity Practices for AI, ENISA, June 2023, available at: https://www.enisa.europa.eu/publications/multilayer-framework-for-good-cybersecurity-practices-for-ai
[34] Cybersecurity of AI and Standardisation, ENISA, March 2023, https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation

- The systems, tools and services developed under this topic will be made available for licencing to national and/or Cross-Border Cyber Hubs platforms, CSIRTs, competent authorities, and other relevant authorities under favourable market conditions.
- These actions aim at providing AI powered cybersecurity capabilities for national and/or Cross-Border Cyber Hubs and for national authorities encompassing cyber hubs, CSIRTs, which occupy a central role in ensuring the cybersecurity of national authorities, providers of critical infrastructures and essential services. These entities are tasked with monitoring, understanding and proactively managing cybersecurity threats. In light of the crucial operative role of Cyber Hubs for ensuring cybersecurity in the Union, the nature of the technologies involved as well as the sensitivity of the information handled, they must be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control.
- Tools to protect and secure AI solutions in line with the EU legislative framework.
- Contribute to the cybersecurity certification of AI-driven cybersecurity solutions and systems. The primary objective of cybersecurity certification for AI systems within the EU is twofold: to mitigate cybersecurity risks inherent in AI technologies and to demonstrate compliance with the EU's comprehensive legislative framework, including the AI Act. By establishing a standardized, transparent, and rigorous certification process, the EU seeks to foster trust in AI technologies among users, developers, and regulators alike.

2.1.3 Deliverables

- Deployment of Artificial Intelligence and various AI/ powered technologies as enablers for Cyber Hubs, CSIRTs, NCSCs, NIS SPOCs and others.
- Novel cybersecurity tools based on AI/ developed, tested and validated in relevant conditions and made available to Cyber Hubs, CSIRTs, NCSCs, NIS SPOCs and others.
- Enhanced information sharing and collaboration amongst national and cross-border Cyber Hubs, CSIRTs, NCSCs, NIS SPOCs and others relevant stakeholders, supported by CTI produced by AI/ powered-tools.
- Tools for automation of cybersecurity processes such as creation, analysis, processing of CTI, to enhance operations of the Cyber Hubs.
- Original European CTI feeds or services.
- Ensure the most advanced and innovative secure AI solutions are developed and implemented for NIS sectors
- Secure AI solutions and tools, complying with EU legislation. Promote the mitigation of risks associated with the misuse of AI by malicious actors, with a focus on AI ethics and secure deployment
- Contribution to the standardisation and certification of cybersecure, trustworthy AI technologies.

Type of action	Simple grant
Indicative budget	*45 mil EUR*
Indicative call planning	2025, 2026, 2027
Indicative duration of the action	3 years
Implementation	ECCC
Type of Beneficiaries	Technology providers, operators of Cyber Hubs Research and academia, cybersecurity entities Public sector, NIS 2 directive entities, private sectors Other relevant stakeholders supporting the deployment of cyber secure AI solutions
Security	Call restricted on the basis of Article 12(5) of the Digital Europe Programme Regulation (EU) 2021/694.

2.2 Strengthening cybersecurity capacities of European SMEs with cybersecure AI powered solutions

2.2.1 Objective

To support the market uptake and dissemination of innovative AI powered cybersecurity solutions (notably in SMEs, possibly using results stemming from Horizon Europe projects or similar) and improve knowledge and auditing of cybersecurity preparedness.

SMEs often lack the resources to assess cyber risks, develop cybersecurity strategies and implement solutions, leaving them vulnerable to cyberattacks. The resilience of organisations that fall into this category is key to the prosperity of the EU single market.

Cyber risk assessment and management can be significantly enhanced and simplified with the application of AI based tools and solutions. However, this requires understanding of the evolving technology landscape, the benefits of technology integration and the prioritisation of the deployment. Faced with organisational and financial constraints, the SMEs may be missing the opportunity to fully harness AI powered solutions to advance their cybersecurity and resilience.

Cybersecurity is the precondition for reliable, secure and resilient AI models and algorithms. Cybersecurity of AI is not just about protecting AI systems against threats such as poisoning and evasion attacks as it also involves ensuring they have trustworthiness features such as human oversight and robustness – the ability to resist cyber-attacks, as required by the EU's AI Act for high-risk AI systems. The need for human oversight of AI has also been emphasized by experts. Also, the use of AI at the SME level supporting the integration of predictive algorithms can greatly support to a bottom-up approach when dealing with vulnerability detections, threat mitigation and more efficient coordinated incident response.

2.2.2 Scope

This action aims to increase the maturity of cyber risk management and improve the cyber resilience and ultimately foster a technologically advanced culture of cybersecurity for the SMEs in the EU. Actions in this topic should develop and deploy AI powered products, tools and services for European SMEs.

Proposals should cover the development or adaptation of the software/hardware and the validation of the solutions.

It foresees the automation of fundamental cybersecurity processes, in particular in small market organisations, through a SaaS toolkit tailored to the needs of SMEs. This toolkit should allow the SMEs to improve the key aspects of their cybersecurity by providing user-friendly tools for risk management[35], threat detection, incident response and notification, to improve their cyber hygiene and mitigate potential threats while protecting personal data. The cyber toolkit should also provide cyber incidents prediction and response functions to improve SME resilience.

Activities should include at least one of the following:

- Uptake/adoption of AI powered cybersecurity tools in organisations where this has not yet taken place.
- Development of user-friendly set of tools (e.g. toolkit) based on AI to automate main cybersecurity processes in SMEs. Such a toolkit could provide automated functions such as:
- A function that supports the assessment and management of an SME's cybersecurity risks. This function should perform a risk assessment, provide recommendations for risk mitigation, and identify options.
    - An interface to existing tools that support the analysis and assessment of the extent of an SME's cyber risk based on information gathered from digital infrastructure scanning and data provided by authorised users.
- A function that issues alerts on relevant vulnerabilities and threats based on the information collected by the risk management function.
- A function that connects SMEs to a Cyber Hub to report an incident and assist with recovery if possible.
- SME user interface for incident reporting associated with the cyber toolkit. Users can report an incident, get instructions on how to react and obtain information on how to obtain support for the response, with the use of AI assistants.

[35] Interoperable EU Risk Management Framework, ENISA, 2023, available at: https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework

2.2.3 Deliverables

- Support the adoption of market-ready innovative AI powered cybersecurity solutions, including solutions developed in the framework of EU-supported research and innovation projects.
- Provide and deploy up to date AI powered tools and services to organisations (in particular SMEs) to prepare, protect and respond to cybersecurity threats.
- Integrate AI technologies into cybersecurity processes to improve the security of ICT solutions.
- Deployment of cybersecure tools and technologies relying on AI; Integration of tools to protect and secure AI solutions.

Type of action	SME support action
Indicative budget	*20 mil EUR*
Indicative call planning	2026
Indicative duration of the action	3 years
Implementation	ECCC
Type of Beneficiaries	SMEs, start-ups, research and academia Public sector, NIS 2 directive entities Other industry actors and related stakeholders
Security	Call restricted based on Article 12(5) of the Digital Europe Programme Regulation (EU) 2021/694.

Deployment of Post-quantum Cryptography

The advances in quantum technologies[36], while bringing positive impact in several sectors of our society, may also have a significant negative impact on cybersecurity. Quantum computers, with their unprecedented computational power, will soon have the potential to break current asymmetric cryptographic protocols and weaken current symmetric ones. With their advent, the known algorithms Rivest-Shamir-Adelman (RSA) and Elliptic Curve Cryptography (ECC), on which many tasks of asymmetric cryptography are based, will be potentially broken in a very short amount of time, probably in a few minutes or days.

Many of the electronic devices and systems in production today could have lifetimes that span 10 years or more, extending into the timeframe when quantum computers are anticipated to be in commercial use. Moreover, when data is captured and stored today, it could be decoded

[36] Quantum Technologies and Cybersecurity, Technology, governance and policy challenges, CEPS report, December 2023, available at: https://www.ceps.eu/ceps-publications/quantum-technologies-and-cybersecurity/

offline later when quantum computers become available. Therefore, the time that sensitive data needs to remain confidential needs to be considered as well.

The whole digital infrastructure is impacted by such threat. This makes it necessary for Europe to look for stronger safeguards for the new quantum digital era, ensuring the confidentiality and integrity of our communications and data, and the authenticity of data as well as of individuals and entities. A transition for asymmetric cryptography to Post-Quantum Cryptography (PQC) is needed. As it is mainly a software-based solution, it is at present the technology that appears as the most promising to be readily deployed as countermeasure to quantum threats.

The transition to PQC[37,38] requires a complete re-thinking and updating of widely deployed software libraries and applications, various hardware features, new protocols, industry best practices, etc.

Post-quantum algorithms are currently being standardized[39] and will continue to be standardized in the near future. However, they may arrive with unknown interoperability and performance issues or side-channel vulnerabilities. Starting tests in Europe for PQC deployment is of utmost importance for the well-functioning of our society, for preparing it for the full transition to PQC, as it can help to identify and address unforeseeable technical and logistic challenges.

Ensuring connectivity and interoperability between organizations, entities, and products from diverse vendors will be a significant challenge during the shift to quantum-resistant algorithms. It is therefore critical to have facilities that allow entities to test PQC implementations and begin planning for the replacement of hardware, software, and systems reliant on pre-quantum public-key algorithms. Also, the creation of collaboration platforms for testing, shared between SMEs, start-ups, public organizations, academia, PQC product suppliers and service providers, and larger corporations, will allow to accelerate the transition of all European actors and will help bring trustworthy PQC solutions to market, benefiting from the innovation of all relevant actors.

At the same time, the successful incorporation of PQC algorithms into existing Public Key Infrastructures (PKIs) is paramount. Core functions such as key establishment, digital

[37] Where Is the Research on Cryptographic Transition and Agility? Gaps facing the industry as quantum safe algorithms move closer to standardization, David Ott, Kenny Paterson, and Dennis Moreau, April 2023, VOL. 66, NO. 4, COMMUNICATIONS OF THE ACM, available at: https://dl.acm.org/doi/pdf/10.1145/3567825

[38] Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms, NIST Cybersecurity White Paper, 2021, Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf

[39] Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography, August 2024, https://csrc.nist.gov/News/2024/postquantum-cryptography-fips-approved

signatures, and protocols must be meticulously adapted with post-quantum equivalents to safeguard against the emerging threats posed by quantum-enabled adversaries.

Finally, Cyber-hubs, both National and cross-border, should lead by example in the EU efforts for deploying PQC.

2.3 Deployment of a European testing infrastructure for the transition to PQC in different usage domains

2.3.1 Objective

This topic supports the creation of a world reference, European testing infrastructure for the transition to PQC, accessible to different kind of actors to perform real-case testing and identification of challenges in the deployment of PQC systems, with a focus on connectivity, interoperability, and agility. Security testing should also be considered, building on the results of other EU-funded projects and activities already ongoing in the EU. The testing infrastructure should be open to European SMEs, start-ups, vendors, and academics for better supporting the design of tests and evaluation of results, as well as to public organizations and to members of large European industry organizations for facilitating exchanges with those actors who have already started their tests. This topic should support the transition of both public and private entities to PQC and to facilitate the emergence of the European market of PQC products, tools and services.

2.3.2 Scope

Proposals are expected creating and maintaining a European PQC testing infrastructure. The testing infrastructure should offer a physical space for in-situ testing, possibly centralised or distributed at different locations in Europe. This includes the possibility for providing remote testing for different European stakeholders in the public and private sector, to perform real-case testing and identification of challenges, with a focus on connectivity, interoperability, agility and security testing. Proposals should build on results from ongoing activities in the EU.

The PQC testing infrastructure should ensure the necessary facilities and the availability of state-of-the-art tools for allowing European users to test PQC deployments in a trusted environment and should facilitate and support access by European industry, with specific focus to SMEs. The infrastructure governance should ensure fairness in the access to the facilities by different users, and data management practices.

A major challenge to be addressed is maintaining connectivity and interoperability among organizations and entities and among products from different vendors during the transition to quantum-resistant algorithms.

The activity should encourage the development of modular and adaptable solutions demonstrating how to apply standards and best practices using commercially available technology.

Activities can also foresee the testing of innovative solutions, such as the combination of high-quality Quantum Random Number Generators (QRNGs) and PQC and should help in achieving a successful market adoption of such solutions.

Activities should include:

- Setting up of a physical space for in-situ testing, offering the possibility of remote testing, including the purchase of necessary tools, novel products and services.
- Design and implementation of real-case tests, with a focus on connectivity, interoperability, and agility, to develop an understanding of the operating conditions of protocols for the applications and of the constraints that may affect use of the products.
- Identification of the needs for replacement/updating hardware, software, and services that use PQC.
- Development of an effective governance mechanism defining the priorities of the service offered and a transparent management process for granting access to users.
- Development or adaptation of the required software/hardware and the validation of the solutions, including open-source libraries with hybrid solutions, which support both the combination of pre-quantum and post-quantum schemes for security reasons, and the backward compatibility with their pre-quantum versions.
- Definition of the access conditions and, development of a catalogue of tests, and services, including efforts for automating conformance testing and security testing.
- Development and deployment of tools that can support the implementation of the European PQC transition roadmap, either for public administrations or other specific sectors; the tools should be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt foreign influence and control.

Proposals are welcome by consortia constituted by European industry players, with eventual participation of public organizations, and academics in the field of applied cryptography.

Participation of non-EU entities entails the risk of highly sensitive information about security infrastructure, risks and incidents being subject to legislation or pressure that obliges those non-EU entities to disclose this information to non-EU governments, with an unpredictable security risk. Therefore, this topic is subject to Article 12(5) of Regulation (EU) 2021/694.

2.3.3 Expected Outcomes

- Trusted, world reference, testing PQC infrastructure, with the necessary facilities and the availability of state-of-the-art tools for allowing users of the infrastructure to fully test all aspects related to trusted PQC deployments.

- A suite of integration tests and end-to-end tests and a suite for automated tests to catch any problematic functioning issues of PQC products early and suggest corrective actions.
- A portfolio of tools that can support connectivity and interoperability tests.
- A framework with a modus operandi allowing to test PQC for a wide variety of contexts and usage domains and allowing the identification of dependencies between issues related to hardware, libraires, protocols and applications.
- Automated security evaluations of software for correctness and resistance to remote side-channel attacks and testing catalogues to assess security against local implementation attacks.
- User-friendly tools, open-source libraries, and secure hardware implementations for PQC.
- Deployment of crypto-agile approaches in the proposed solutions.
- Enhancement and consolidation of capabilities in PQC roll-out in different domains.
- Regular publication of reports on the outcomes including successful and failed interoperability tests as well as issues and challenges identified.
- Results on testing innovative solutions, combining technologies of different types, such as new QRNGs and PQC.

Type of action	Procurement
Indicative budget	*25 mil EUR*
Indicative call planning	2025
Indicative duration of the action	4 years
Implementation	ECCC
Type of Beneficiaries	SMEs, start-ups, public organizations, research, academia and providers of post-quantum solutions and services, other industry actors
Eligibility	Article 12.5

2.4 Transition to post-quantum Public Key Infrastructures

2.4.1 Objectives

The overarching aim of this call is to tackle the challenges of an effective integration of PQC algorithms in Public Key Infrastructures (PKIs), which guarantees, at the same time, backward compatibility with the current PKIs.

The call targets the different actors involved in the PKI ecosystems and supply and value chains, who all have a unique set of diverse needs and interdependencies, such as Certificate Authorities (CAs), intermediate CAs, researchers, end-users in different domains, and vendors.

2.4.2 Scope

Proposals shall target activities on the following subjects:

- design of digital signature combiners and key encapsulation mechanism combiners.
- the testing of deployment of certificates in protocols that use those certificates.
- the development of novel protocols for Automatic Certificate Management and revocation and of novel protocols for (privacy-friendly) certificate-transparency.
- the development of methods and tools that can be used by experts across various PKI domains, including all aspects of key management of asymmetric systems.

Proposals should carefully consider the requirements and constraints, such as security level, performance and backward compatibility, in a broad range of applications relevant for critical societal sectors and processes (such as governmental services, telecom, banking, smart homes, e-Health, automotive, others).

Proposals should address functions such as key establishment, digital signatures, and secure communication protocols that require careful adaptation with post-quantum counterparts to ensure resilience against threats posed by quantum-capable adversaries.

Proposals should safeguard compatibility with existing legacy systems. To achieve this, a transition to PKIs that support both pre-quantum and post-quantum cryptography should be addressed, combining pre-quantum and post-quantum key encapsulation and digital signature algorithms. The proposed systems should be able to seamlessly interact with legacy systems by disabling the post-quantum component as needed while preventing downgrade attacks.

For certificates for protocols that support negotiation, such as X.509 certificates for the Transport Layer (TLS), the use of post-quantum key exchange has already been demonstrated and can be implemented in a decentralized manner. Many other protocols need to be migrated, and this process will be more complex when old and new configurations must coexist. Moreover, for applications in IoT, smartcards, identity documents and others, the migration strategies defined for the core use cases of X.509 may well not work.

Proposals should develop clear procedures to effectively guide the various stakeholders involved in PKIs across different usage domains through the transition process.

Effective consortia should comprise a diverse range of actors along the entire PKI chain, encompassing expertise in areas such as software development, hardware implementation, cryptographic research, policy, and application deployment, as well as organizations that can provide user case studies and real-world applications.

Activities should include some or all of the following:

- Identification of requirements necessary to implement hybrid certificates.
- Development of approaches and techniques for constructing cryptographic combiners for different protocols.
- Testing of the combiners for issuance of new certificates for the different applications, taking into consideration the need to balance the growth of key, signature, and ciphertext sizes, which can lead to compatibility issues with standards, such as PKI certificates, revocation mechanisms, (privacy-friendly) certificate transparency mechanisms, the use of different cryptographic protocols across certificate chains, the applications requirements, such as security level, time-constraints in signing and verification steps, communication/computational and storage overhead, and hardware optimization requirements.
- Development of and/or further improvement of open-source libraries.
- Development of novel protocols for Automatic Certificate Management and revocation and of novel protocols for (privacy-friendly) certificate-transparency.
- Development of recipes for the design and deployment of the new PKIs, with analysis that depends on each component of a given PKI.
- Tests on specialized uses of X.509 certificates other than the core cases using TLS, such as roots of trust, device integrity, firmware signing, and others.
- Design, improvement and testing of X.509 alternatives, such as, among others, Merkle tree ladders, the GNU Name System, older proposals such as SPKI and SDSI and the use of key encapsulation mechanisms for on-demand authentication in place of signatures.
- Awareness and training activities for stakeholders with different profiles, emphasizing the interdependencies in the transition and facilitating a broader understanding of the technical standards amongst PKI users.
- Participation of non-EU entities entails the risk of highly sensitive information about security infrastructure, risks and incidents being subject to legislation or pressure that obliges those non-EU entities to disclose this information to non-EU governments, with an unpredictable security risk. Therefore, based on the outlined security reasons, this topic is subject to Article 12(5) of Regulation (EU) 2021/694.

2.4.3 Expected Outcomes

- New combiners ensuring that cryptographic schemes provide at least 128-bit security against quantum adversaries.
- Experimental evaluation on hybrid certificates in several standard protocols that use those certificates, also considering options for different cryptographic algorithms at the root Certification Authority level and at the other levels, in terms of security, performance, and backward compatibility. The impact of such certificates in protocols should be tested via open source libraries.

- New and/or improved open-source libraries for certificate requests, issuance, validation, revocation and (privacy-friendly) certificate transparency.
- Clear procedures taking into account all aspects of key management: requirements for signature generation, in terms of the software and hardware used to create signatures as well as the secure storage and handling of private keys to maintain their authenticity and confidentiality, signature validation, with specification of the data required for verifying signatures and outlining the conditions necessary for a successful signature verification process, signature life-cycle process, and validity status of signatures.
- Test and evaluation of uses of X.509 certificates other than their core uses.
- Tests and evaluation of alternatives to X.509 certificates.
- Awareness activities and trainings.

Type of action	Simple grant
Indicative budget	*15 mil EUR, (grant of 4 to 5 mil)*
Indicative call planning	2025
Indicative duration of the action	3 years
Implementation	ECCC
Type of Beneficiaries	All actors in PKI chain
Security	Call restricted based on Article 12(5) of the Digital Europe Programme Regulation (EU) 2021/694.

2.5 Migration of Cyber-hubs to PQC

2.5.1.1 Objective

The overarching aim is to integrate PQC products, components, systems, protocols, and services into the existing digital security and communication networks of national and cross-border Cyber-hubs. Cyber-hubs should proactively adopt PQC, and work towards a seamless and timely integration of PQC into their digital infrastructures and services.

Activities on the adoption of PQC by Cyber-Hubs should foster a wider collaboration and coordination to ensure operational continuity during testing of PQC solutions.

2.5.1.2 Scope

Proposals should target the deployment of PQC systems, tools and services in national and cross-border Cyber-hubs. Proposals should include testing for the seamless integration of PQC in secure communication between Cyber-Hubs, across the protocols used by such entities, like TLS (used for HTTPS), VPNs, and digital signatures. Proposals should cover the development or adaptation of the required software/hardware and the validation of the solutions, also liaising their activities with ENISA, for ensuring compliance with the validation and certification schemes developed by the ECCG. Proposals should identify vendors providing software or

other products used by the Cyber-hubs, as well as vendors that handle hosting, storage, processing of data, security accreditations and certification.

Proposals should ensure that implementations are crypto-agile, such that cryptographic algorithms and modules can be easily upgraded or replaced without having to completely replace the underlying application or device. Crypto-agility shall be considered also in terms of compliance and security strength, meaning the capacity to adapt cryptographic configurations in accordance with compliance requirements and the capability to dynamically adjust the security level based on configuration, allowing for scalable security measures. Solutions implemented should allow for backward compatibility with pre-quantum solutions.

Representative examples of activities that proposals could cover include:

- Actions to prepare and plan for the PQC transition, in alignment with the actions identified in regular drafts of the Coordinated Implementation Roadmap for the transition to PQC, following the Commission Recommendation issued on 11 April 2024.
- Analysis and evaluation of the vulnerabilities and strengths of the cryptographic foundations of the current e-government applications.
- Deployment of software components, open-source libraries, and hardware components such as Hardware Security Modules and hardware authentication tokens for Multi-Factor Authentication.
- Liaison with ENISA for the work done in the context of the ECCG on certification, and inclusion of service and product providers roadmap in the plan of the activities.
- Deployment and integration of crypto-agile and hybrid PQC solutions (allowing for backward compatibility and supporting the combination of pre-quantum and post-quantum schemes for security reasons) specifically tailored for Cyber-Hubs and e-government applications.
- Establishment of a plan for awareness and involvement of internal staff and external actors interacting with the Cyber-Hubs in training programs.

Proposals are expected by individual Cyber-hubs and can include providers of PQC solutions and services and other relevant stakeholders (public and private).

Participation of non-EU entities entails the risk of highly sensitive information about security infrastructure, risks and incidents being subject to legislation or pressure that obliges those non-EU entities to disclose this information to non-EU governments, with an unpredictable security risk. Therefore, based on the outlined security reasons, the actions relating to these technologies are subject to Article 12(5) of Regulation (EU) 2021/694.

2.5.1.3 Expected Outcomes

- Strategy to implement the actions foreseen in the drafts of the Coordinated Implementation Roadmap for the transition to PQC.

- Deployment of crypto-agile, hybrid (allowing for backward compatibility) solutions, including updated software libraries and hardware components as well as network protocols.
- PQC systems validation and liaison with entities dealing with certification activities.

Type of action	Simple grant
Indicative budget	*7 mil EUR (grant of 1 to 2 mil EUR)*
Indicative call planning	2027
Indicative duration of the action	3 years
Implementation	ECCC
Type of Beneficiaries	Cyber Hubs, competent authorities, providers of PQC solutions and services, other relevant stakeholders (public or private)
Security	Call restricted based on Article 12(5) of the Digital Europe Programme Regulation (EU) 2021/694.

2.6 Uptake of innovative cybersecurity solutions for SMEs

The action also aims at improving industrial and market readiness for the cybersecurity requirements set in the Cyber Resilience Act bolstering cybersecurity rules to ensure more secure hardware and software products.

2.6.1 Objectives

Proposals should contribute to achieving at least one of these objectives:

- Development of trust and confidence between Member States.
- Effective operational cooperation of organisations entrusted with EU or Member State's Cybersecurity, in particular cooperation of Cyber Hubs, CSIRTs (including in relation to the CSIRT Network) and/or ISACs, highly critical and other critical sectors entities.
- Improved security and notification processes and means in the EU.
- Improved security of network and information systems in the EU.
- More alignment of Member States' implementations of the NIS 2 Directive.
- Industrial and market readiness for the proposed Cyber Resilience Act.
- Support Cybersecurity certification in line with the Cybersecurity Act.
- Help manage the growing complexity of the technology landscape by assisting cybersecurity professionals to research vulnerabilities, detect, analyse, and respond to threats.
- Support supply chain partners in standardized self-assessments and certifications. Helping downstream supply chain partners in a step-by-step approach in increasing cyber resilience.

- Overcome the challenge of finding the technical skills required to deal with a complex technology landscape that relies heavily on extensive configurations and capabilities.
- Cyber toolkit as a service to support for SMEs[40] managing cyber risks, defining, and implementing their cybersecurity strategy, including several functions dedicated to risk assessment, vulnerabilities and threats detection, etc.
- Support and incident response capabilities to SMEs, including guidelines, procedures in case of incidents, support tools and platforms.

2.6.2 Scope

The action will focus on the support of at least one of the following priorities listed below, in the next section.

2.6.3 Deliverables

The development of a cyber toolkit as a service to support for SMEs managing cyber risks, defining, and implementing their cybersecurity strategy. The toolkit should include:

- Interfaces to existing cloud-based SaaS applications such as HR, invoice and financial management, customer relationship management and accounting systems, etc., which are often used by SMEs.
- A functionality that enables the mapping and maintenance of an SME's digital assets by interfacing with other SaaS applications that manage an asset inventory and data repositories.
- A function that supports the assessment and management of an SME's cybersecurity risks and of supply chain risk management. This function should perform a risk assessment, provide recommendations for risk mitigation, and identify options.
- An interface to existing tools that support the analysis and assessment of the extent of an SME's cyber risk based on information gathered from digital infrastructure scanning and data provided by authorised users.
- A function that raises awareness, provides training, and informs skills development and training activities[41].
- A function that issues alerts on vulnerabilities and threats based on the information collected by the risk management function.
- A function that connects SMEs to a CSIRT or a Cyber Hub to report an incident and assist with recovery if possible.
- A mapping and one-stop window/portal to existing tools and solutions targeting cybersecurity support to SMEs.

[40] Cybersecurity guide for SMEs - 12 steps to securing your business, ENISA, 2021, available at https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes

[41] On the basis of the ECSF.

- Tools supporting detection, prevention and response in Operational Technology infrastructures using open standards or technologies.
- Automation tools processing advisory information using open standards.
- Best practices and/or policy suggestions to improve cross-border cyber supply chains.

Support and incident response capabilities to SMEs:

- Non-commercial cybersecurity hotline with a standardized framework and guidelines for response times, escalation procedures, and the scope of assistance provided.
- A fully operational, multilingual helpline that provides timely and accurate cybersecurity assistance to SMEs, leading to reduced successful cyber scams and improved digital hygiene.
- A National Cyber Response Platform for first cyber responders to exchange their experiences, share relevant news and engage discussions regarding challenges and emerging cyber threats complementary to existing cyber crisis management structures.
- A pool of cybersecurity experts and volunteers to support incident response actions.
- Specialized training modules for first (public and private) responders' services targeting different sectors such as healthcare, finance, energy, and transportation.

Support tools and platforms:

- Control Centre and Panel on Incident Reporting and dispatching of incident responders.
- SME user interface for Incident reporting associated with the cyber toolkit. Users can report an incident, get instructions on how to react and obtain information on how to receive support for the response. An AI assistant connected to a Control Centre could also be included.
- Interfaces with the National Authorities and Cross-Border Platforms (CBPs) for incident notification and information sharing.

Type of action	SME support action
Indicative budget	15 mil EUR
Indicative call planning	2025
Indicative duration of the action	3 years
Implementation	ECCC
Type of Beneficiaries	SMEs, private and public entities implementing NIS 2 Directive, Cyber Resilience Act, research and academia, etc.
Security	Call for grants and procurement are restricted on the basis of Article 12(5) of the Regulation (EU) 2021/694.

Cyber Solidarity Act Implementation

European Cybersecurity Alert System

In a context of accelerated digitisation as well as the growing number and impact of cybersecurity incidents, the European Commission (EC) adopted in December 2020 the "EU Cybersecurity Strategy for the Digital Decade." Among other objectives, the EU Cybersecurity Strategy aims to improve capacities and cooperation to detect cyber threats, before they can cause large-scale damage, in view to detect more threats and do so much faster.

The EU Cybersecurity Strategy proposes to build, strengthen, and interconnect, across the European Union, Security Operation Centres (SOCs) and Cyber Threat Intelligence (CTI) capabilities (monitoring, detection and analysis), with the aim to support the detection and prevention of cyber threats and the provision of timely warnings to authorities and all relevant stakeholders. Such cyber security capabilities are typically ensured by SOCs in combination with Computer Emergency Response Teams / Computer Security Incident Response Teams (CERTs/CSIRTs), with the support of external, specialised sources of intelligence on cyber threats.

To implement this strategy, the previous DIGITAL work programmes (2021-2022 and 2023-2024) included actions supporting the creation of national SOCs, and networking them at European level via Cross-Border SOC platforms and coordinating their activities to create a stronger SOC ecosystem, also comprising of local and regional, private and public security centres for both horizontal and vertical sectors.

As per the political agreement on the Cyber Solidarity Act to be adopted and publish in the Official Journal[42], it is necessary to strengthen the detection and situational awareness of cyber threats and incidents throughout the Union and to strengthen solidarity by enhancing Member States' and the Union's preparedness and capabilities to prevent and respond to significant, large-scale and large-scale-equivalent cybersecurity incidents.

The Cyber Solidarity Act envisages, as part of the **European Cybersecurity Alert System (ECAS)**, that a pan-European network of Cyber Hubs should be established, to build and enhance coordinated detection and common situational awareness capabilities. It is also envisaged the support for the development and consolidation of the national Cyber Hubs and the Cross-Border Cyber Hubs, that were also financed previously and referred as national SOCs/Cross-border SOCs.

The activities of this work programme build on the work already initiated in previous work programmes, where investment was made to support the creation of national SOCs and their

[42] To be adopted and publish in the Official Journal by the end of 2024.

interlinking via Cross-Border SOCs. While the *Cyber Solidarity Act*[43] brings in new terminology – *Cyber Hubs* and *Cross-Border Cyber Hubs* – as part of the *European Cybersecurity Alert System*, this work programme aims to consolidate previous activities focusing on SOCs, with the objective to support joint actions to create an advanced (state-of-the-art) threat detection and cyber early warning ecosystem remains. This objective allows to reinforce capacities through the coordination of actions on collective knowledge and data sources, bringing together data from multiple sources and expanding cybersecurity threat intelligence. By fostering common and interoperable infrastructures across EU, this will make it possible to share more efficiently and more rapidly the signals detected, thus enabling a better situational awareness and a more rapid and effective reaction. The actions in this work programme are focussed along three strands:

- National Cyber Hubs.
- Cross Border Cyber Hubs.
- Strengthening the Cyber Hubs ecosystem and enhancing information sharing.

The Union financial contribution shall cover up to 75% of the acquisition costs under joint procurement for Cross-Border Cyber Hubs and 50% of the acquisition costs under joint procurement for national Cyber Hubs. In both cases, a hosting and usage agreement will be concluded. Up to 50% of the running costs of national or Cross-Border Cyber Hubs will be covered by a complementing grant. The remaining total cost of ownership of the national and Cross-Border Cyber Hubs shall be covered by the Participating States in the hosting consortium.

Cybersecurity Emergency Mechanism

This section focuses on capacity building and the enhancement of cooperation on cybersecurity at technical, operational and strategic levels, in the context of EU legislation on cybersecurity in particular the NIS 2 Directive[44], the Cybersecurity Act[45] and the proposed Cyber Resilience Act[46] and Cyber Solidarity Act. The proposed actions will support the implementation Cyber Solidarity Act and the establishment of a Cybersecurity Emergency Mechanism designed to support Member States upon their request in preparing for, responding to, and initially recovering from significant and large-scale cybersecurity incidents.

Technical Mutual Assistance

[43] Most recent negotiated versions of the "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents" COM(2023) 209. It is expected to be published during 2024.
[44] See https://eur-lex.europa.eu/eli/dir/2022/2555
[45] See https://eur-lex.europa.eu/eli/reg/2019/881/oj
[46] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0454

A topic dedicated to mutual assistance, steaming from Cyber Solidarity Act is also foreseen.

2.7 National Cyber Hubs

Where a Member State decides to participate in the European Cybersecurity Alert System, it shall designate or, where applicable, establish a national Cyber Hub, a single entity acting under the authority of the Member State.

National Cyber Hubs have the capacity to act as a reference point and gateway to other public and private organisations at national level for collecting and analysing information on cyber threats and incidents and to contribute to a Cross-Border Cyber Hub. They are capable of detecting, aggregating, and analysing data and information relevant to cyber threats and incidents, such as cyber threat intelligence, by using in particular state-of-the-art technologies, and with the aim to prevent incidents.

As already mentioned, for the following programming cycle, the emphasis is on continuation of activities initiated during past years.

2.7.1 Objective

The objective is to create or strengthen national Cyber Hubs, with state-of-the-art tools for monitoring, understanding and proactively managing cyber events, in close collaboration with relevant entities such as CSIRTs, ISACs, etc. They will also, where possible, benefit from information and feeds from other Cyber Hubs in their countries and use the aggregated data and analysis to deliver early warnings to targeted critical infrastructures on a need-to-know basis.

2.7.2 Scope

The aim is capacity building for new or existing national Cyber Hubs, e.g., equipment, tools, data feeds, as well as costs related to data analysis, interconnection with Cross-Border Cyber Hubs, etc. This can include for example automation, analysis and correlation tools and data feeds covering Cyber Threat Intelligence (CTI) at various levels, ranging from field data to Security Information and Event Management (SIEM) data to higher level CTI. Automation is a key aspect in the efficient handling and processing of information. Where available, already established standards should be used like the Common Security Advisory Framework (CSAF)[47] for security advisories or collecting and processing of cybersecurity related messages (e.g. by the IntelMQ project[48]). Applications developed by Cyber Hubs/SOCs should be compatible with European standardisation projects like the EU vulnerability database (EUVD). National

[47] Common Security Advisory Framework (CSAF): Machine-processable format enables automated database reconciliation - https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/CSAF/CSAF_node.html

[48] IntelMQ: https://github.com/certtools/intelmq

Cyber Hubs should also leverage state of the art technology such as artificial intelligence and dynamic learning of the threat landscape and context. This also includes the use of shared cybersecurity information, to the extent possible based on existing taxonomies and/or ontologies, and hardware to ensure the secure exchange and storage of information. The operations should be built upon live network data and other training data required in the initial phases. Where relevant, consideration should be given to SMEs as the ultimate recipients of cybersecurity operational information.

A key element is the translation of advanced AI, data analytics and other relevant cybersecurity tools from research results to operational tools, and further testing and validating them in real conditions in combination with access to supercomputing facilities (e.g., to boost the correlation and detection features of cross-border platforms). Such activities are identified and proposed for financing in section 2.3, dedicated to AI for Cybersecurity, and topic 2.3.1.

Another key role for national Cyber Hubs is knowledge transfer and sharing, such as training of cybersecurity analysts on the basis, for instance, of the European Cybersecurity Skills Framework (ECSF[49]). For example, Cyber Hubs/SOCs dealing with critical infrastructures play a key role and should benefit from the knowledge and experience acquired by or concentrated in national Cyber Hubs.

National Cyber Hubs must share information with other stakeholders in a mutually beneficial exchange of information and commit to apply to participate in a Cross-Border Cyber Hub within the next 2 years, with a view to exchanging information with other national Cyber Hubs.

To achieve this aim, a call for expression of interest[50] will be launched to select entities in Member States that provide the necessary facilities to host and operate national Cyber Hubs. Applicants to the call for expressions of interest should describe the aims and objectives of the national Cyber Hubs, describe its role and how such role relates to other cybersecurity actors, such as CSIRTs, and its eventual cooperation with other public or private cybersecurity stakeholders. Applicants should also provide the detailed planning of the activities and tasks of the national Cyber Hubs, the services it will offer, the way they will operate and be operationalised, and describe the duration of the activity as well as the main milestones and deliverables. They should also specify what equipment, tools and services need to be procured and integrated to build up the national Cyber Hubs, its services and its infrastructure.

To support the above activities of a national Cyber Hub, the following two workstreams of activities are foreseen:

[49] https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

[50] Please note this is not a call for expression of interest within the meaning of Point 13 of Annex I of the Regulation (EU, Euratom) 2018/1046. The aim is to select the future contracting authorities taking part in a joint procurement.

- **[Procurement] A Joint Procurement Action** with the Member State where the national Cyber Hub is located: this will cover the procurement of the main infrastructure, tools and services needed to build up the national Cyber Hub.
- **[Building up and running the national Cyber Hubs]** A grant will also be available to cover, among others, the preparatory activities for setting up the national Cyber Hubs, its interaction and cooperation with other stakeholders, as well as the running/operating costs involved, enabling the effective operation of the national Cyber Hubs, e.g., using the infrastructure, tools and services purchased through the joint procurement. These will also indicate milestones and deliverables to monitor progress.

Applications shall be made to both workstreams. Applications will be object of evaluations procedures. Grants will only be awarded to applicants that have succeeded in the evaluation of the joint procurement action.

These actions aim at creating or strengthening national Cyber Hubs, which occupy a central role in ensuring the cybersecurity of national authorities, providers of critical infrastructures and essential services. Cyber Hubs are tasked with monitoring, understanding and proactively managing cybersecurity threats. Cyber Hubs will have a crucial operative role for ensuring cybersecurity in the Union and will handle sensitive information.

The choice of the security option will depend on the result, and will be based on, the mapping to be issued by the ECCC in accordance with Article 9(4) of Cyber Solidarity Act.

The mapping comprises the tools, infrastructures or services necessary and of adequate quality to establish, or enhance the capabilities of, National Cyber Hubs and Cross-Border Cyber Hubs, their availability, including from legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States.

Please note that once the Cyber Solidarity Act is adopted and published in the Official Journal and the mapping of services needed for the European Cybersecurity Alert System in accordance with the Cyber Solidarity Act is concluded, the WP text will be amended, where appropriate, to reflect the results of the assessment and to set the security conditions accordingly (for National and Cross-Border Cyber Hubs).

2.7.3 Deliverables

World-class national Cyber Hubs across the Union, strengthened with state-of-the-art technology, acting as clearinghouses for detecting, gathering and storing data on cybersecurity threats, analysing this data, and sharing and reporting CTI, reviews and analyses taking into account well-established standards for sharing and automation processes.

Threat intelligence and situational awareness capabilities and capacity building supporting strengthened collaboration between cybersecurity actors, including private and public actors.

- Targeted trainings on the basis of the ECSF to improve the capacity of cyber security analysts.
- Applications for automated notification of private and public actors about compromised or insecure systems.

Type of action	Call for Expression of Interest - workstream on Joint procurement with Member States
Indicative budget	*35 mil EUR*-- The Authorising Officer by Delegation shall adapt the amounts for the actions set out in section 2.7 based on the amounts requested in the submissions received.
Indicative call planning	2025, 2026
Indicative duration of the action	3 years
Implementation	ECCC
Type of Beneficiaries	Public bodies acting as national Cyber Hubs, as identified by Member States
Security	The choice of the security option will depend on the result, and will be based on, the mapping to be issued by the ECCC in accordance with Article 9(4) of the Cyber Solidarity Act. The mapping comprises the tools, infrastructures or services necessary and of adequate quality to establish, or enhance the capabilities of, National Cyber Hubs and Cross-Border Cyber Hubs, their availability, including from legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States.[51]. Further explanation on Grants and Procurement conditions relevant for security is provided in the 'third country participation' and 'procurement from non-EU entities' paragraphs of this document.

Type of action	Call for Expression of Interest - workstream on Simple Grants
Indicative budget	*To be defined*-- The Authorising Officer by Delegation shall adapt the amounts for the actions set out in section 2.7 based on the amounts requested in the submissions received.
Indicative call planning	2025, 2026
Indicative duration of the action	3 years
Implementation	ECCC
Type of Beneficiaries	Successful applicants to the workstream on joint procurement

[51] Once the Cyber Solidarity Act is adopted and publish in the Official Journal and the mapping of services needed for the European Cybersecurity Alert System in accordance with the Cyber Solidarity Act is concluded, the WP text will be amended, to reflect the results of the assessment and to set the security conditions accordingly (for National and Cross-Border Cyber Hubs),

Security	The choice of the security option will depend on the result, and will be based on, the mapping to be issued by the ECCC in accordance with Article 9(4) of the Cyber Solidarity Act. The mapping comprises the tools, infrastructures or services necessary and of adequate quality to establish, or enhance the capabilities of, National Cyber Hubs and Cross-Border Cyber Hubs, their availability, including from legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States.[52]. Further explanation on Grants and Procurement conditions relevant for security is provided in the 'third country participation' and 'procurement from non-EU entities' paragraphs of this document.

Type of action	Administration, Simple Grant
Indicative budget	*3,343,961.00 EUR*-- The Authorising Officer by Delegation shall provide the amount for the action from the amount set out in section 2.7.
Indicative call planning	2025
Implementation	ECCC
Type of Beneficiaries	Budgetary appropriation for a grant under preparation from the ongoing WP2022 call DIGITAL-ECCC-2022-CYBER-B-03-SOC - Capacity building of Security Operation Centres (SOCs). Budget: 3,343,961.00.

2.8 Cross-Border Cyber Hubs

The former Cross-border SOC platforms were financed during previous calls and such collaboration is envisaged for the Cross-Borders Cyber Hubs. They should provide new additional capacity building upon and complementing existing SOCs/Cyber Hubs, Computer Security Incident Response Teams (CSIRTs), ISACs and other relevant actors.

2.8.1 Objective

This action aims at new Cross-Border Cyber Hubs, as well as supporting the SOCs that were already launched under the previous DIGITAL work programmes (2021-2022 and 2023-

[52] Once the Cyber Solidarity Act is adopted and publish in the Official Journal and the mapping of services needed for the European Cybersecurity Alert System in accordance with the Cyber Solidarity Act is concluded, the WP text will be amended, to reflect the results of the assessment and to set the security conditions accordingly (for National and Cross-Border Cyber Hubs),

2024)[53]. In addition to setting up processes, tools and services for prevention, detection and analysis of emerging cyber-attacks, the scope also covers the acquisition and/or adoption of common (automation) tools, processes and shared data infrastructures for the management and sharing of contextualised and actionable cybersecurity operational information across the EU. Well-established open standards for CTI sharing (e.g. MISP Standard[54]) or automation of advisory information (e.g. CSAF[55]) and cybersecurity related messages (e.g. by IntelMQ) should be considered.

2.8.2 Scope

The Cross-Border Cyber Hubs platforms will contribute to enhancing and consolidating collective situational awareness and capabilities in detection and CTI, supporting the development of better performing data analytics, detection, and response tools, through the pooling of large amounts of data, including new data generated internally by the consortia members.

The platforms should act as a central point allowing for broader pooling of relevant data and CTI, enable the spreading of threat information on a large scale and among a large and diverse set of actors (e.g., CERTs/CSIRTs, ISACs, operators of critical infrastructures).

According to the Cyber Solidarity Act, the Cross-Border Cyber Hubs and the CSIRTs Network shall cooperate closely, in particular for the purpose of sharing information. To that end, they shall agree on procedural arrangements on cooperation and sharing of relevant information and the types of information to be shared.

Where the Cross-Border Cyber Hubs obtain information relating to a potential or ongoing large-scale cybersecurity incident, they shall ensure, for the purpose of common situational awareness, that relevant information as well as early warnings are provided to Member States' authorities and the Commission through EU-CyCLONe and the CSIRTs network[56], without undue delay. A call for expression of interest will be launched to select entities in Member States that provide the necessary facilities to host and operate Cross-Border Cyber Hubs for pooling data on cybersecurity threats between several Member States. Applicants to the call for expressions of interest should describe the aims and objectives of the Cross-Border Cyber Hub, describe its role and how such role relates to other cybersecurity actors, and its eventual cooperation with other public or private cybersecurity stakeholders. Applicants should also provide the detailed planning of the activities and tasks of the Cross-Border Cyber Hub, the

[53] ENSOC and ATHENA consortia are already financed.
[54] MISP Standard: https://www.misp-standard.org/
[55] Common Security Advisory Framework (CSAF): Machine-processable format enables automated database reconciliation - https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/CSAF/CSAF_node.html
[56] As defined by Directive (EU) 2022/2555.

services it will offer, the way they will operate and be operationalised, as well as the main milestones and deliverables. They should also specify what equipment, tools and services need to be procured and integrated to build up the Cross-Border Cyber Hub, its services and its infrastructure.

To support the above activities of a Cross-Border Cyber Hub, the following two workstreams of activities are foreseen:

- **[Procurement] A Joint Procurement Action** with the Member State participating in the Cross-Border Cyber Hub: this will cover the procurement of the infrastructure, tools and services needed to build up the Cross-Border Cyber Hub.
- **[Building up and running the Cross-Border Cyber Hub]** A grant will also be available to cover, among others, the preparatory activities for setting up the Cross-Border Cyber Hub, its interaction and cooperation with other stakeholders, as well as the running/operating costs involved, enabling the effective operation of the Cross-Border Cyber Hub, e.g., using the infrastructure, tools and services purchased through the joint procurement. These will also indicate milestones and deliverables to monitor progress.

Applications shall be made to both workstreams. Applications will be object of evaluations procedures. Grants will only be awarded to applicants that have succeeded the evaluation of the joint procurement action.

These actions aim at creating or strengthening Cross-Border Cyber Hubs, which occupy a central role in ensuring the cybersecurity of national authorities, providers of critical infrastructures and essential services. As previously noted, Cyber Hubs will have a crucial operative role of Cyber Hubs for ensuring cybersecurity in the Union and will handle sensitive information. The choice of the security option will depend on the result, and will be based on, the mapping to be issued by the ECCC in accordance with Article 9(4) of the Cyber Solidarity Act.

The mapping comprises the tools, infrastructures or services necessary and of adequate quality to establish, or enhance the capabilities of, National Cyber Hubs and Cross-Border Cyber Hubs, their availability, including from legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States.

Please note once the Cyber Solidarity Act is adopted and published in the Official Journal and the mapping of services needed for the European Cybersecurity Alert System in accordance with the Cyber Solidarity Act is concluded, the WP text will be amended to reflect the results of the assessment and to set the security conditions accordingly (for National and Cross-Border Cyber Hubs).

2.8.3 Deliverables

- World-class Cross-Border Cyber Hubs across the Union for pooling data on cybersecurity threats between several Member States, equipped with a highly secure

infrastructures and advanced data analytics tools for detecting, gathering and storing data on cybersecurity threats, analysing this data, and sharing and reporting CTI, reviews and analyses.

- Sharing of Threat Intelligence between national Cyber Hubs, and information sharing agreements with competent authorities and networks, including CSIRTs.

Type of action	Call for Expression of Interest – workstream on Joint procurement with Member States
Indicative budget	*40 mil EUR*--The Authorising Officer by Delegation shall adapt the amounts for the actions set out in section 2.1.2 based on the amounts requested in the submissions received.
Indicative call planning	2025, 2027
Indicative duration of the action	3 years
Implementation	ECCC
Type of Beneficiaries	Public bodies acting as national Cyber Hubs, as identified by Member States.
Security	The choice of the security option will depend on the result, and will be based on, the mapping to be issued by the ECCC in accordance with Article 9(4) of the Cyber Solidarity Act. The mapping comprises the tools, infrastructures or services necessary and of adequate quality to establish, or enhance the capabilities of, National Cyber Hubs and Cross-Border Cyber Hubs, their availability, including from legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States[57]. Further explanation on Grants and Procurement conditions relevant for security is provided in the 'third country participation' and 'procurement from non-EU entities' paragraphs of this document.

Type of action	Call for Expression of Interest – workstream on Simple Grants
Indicative budget	*To be defined*--. The Authorising Officer by Delegation shall adapt the amounts for the actions set out in section 2.1.2 based on the amounts requested in the submissions received.
Indicative call planning	2025, 2027
Indicative duration of the action	3 years
Implementation	ECCC
Type of Beneficiaries	Successful applicants to the workstream on joint procurement

[57] Once the Cyber Solidarity Act is adopted and publish in the Official Journal and the mapping of services needed for the European Cybersecurity Alert System in accordance with the Cyber Solidarity Act is concluded, the WP text will be amended, to reflect the results of the assessment and to set the security conditions accordingly (for National and Cross-Border Cyber Hubs).

Security	The choice of the security option will depend on the result, and will be based on, the mapping to be issued by the ECCC in accordance with Article 9(4) of the Cyber Solidarity Act. The mapping comprises the tools, infrastructures or services necessary and of adequate quality to establish, or enhance the capabilities of, National Cyber Hubs and Cross-Border Cyber Hubs, their availability, including from legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States[58]. Further explanation on Grants and Procurement conditions relevant for security is provided in the 'third country participation' and 'procurement from non-EU entities' paragraphs of this document.

2.9 Strengthening the Cyber Hubs ecosystem and enhancing information sharing

This topic complements the previous actions on national Cyber Hubs and the Cross-Border Cyber Hubs and aims to consolidate them including the ones in selected consortia, ENSOC and ATHENA, which engaged in joint procurement with the ECCC to purchase the necessary tools and infrastructures to establish the cross-border SOC platforms.

These actions should lead to increased engagement, including from the private sector, and to a better collaboration towards a common EU cyber threat knowledge base and technological independence.

2.9.1 Objectives

Actions should address one or more of the following:

- Supporting the cooperation and coordination of Cross-Border Cyber Hubs, both between different Cross-Border Cyber Hubs, and with relation to national Cyber Hubs and other Cyber Hubs, and in the absence of cyber hubs relevant Member State authorities.
- Fostering links between public sector and industry, and stimulate mutually beneficial exchange of information, tools and data as well as exchange of knowledge and training opportunities.

[58] Once the Cyber Solidarity Act is adopted and publish in the Official Journal and the mapping of services needed for the European Cybersecurity Alert System in accordance with the Cyber Solidarity Act is concluded, the WP text will be amended, to reflect the results of the assessment and to set the security conditions accordingly (for National and Cross-Border Cyber Hubs).

- Fostering links between Cyber Hubs and industrial stakeholders in artificial intelligence and in other enabling technologies, fostering the adoption of such technologies, including AI techniques (such as for example those developed in Sections 2.1-2.6 of this work programme dedicated to AI and post quantum technologies) and knowledge exchange.
- Supporting the notification on compromised or insecure systems as part of the coordinated vulnerabilities disclosure between relevant national authorities as included in the NIS 2 Directive.
- Facilitating Operational Technology detection, prevention and response considering open standards or technologies.

As previously noted, Cyber Hubs will have a crucial operative role of Cyber Hubs for ensuring cybersecurity in the Union and will handle sensitive information. Therefore, the actions relating to Cyber Hubs are subject to Article 12(5) of Regulation (EU) 2021/694.

2.9.2 Deliverables

- Events, workshops, stakeholder consultations, architectural designs and white papers on technical coordination and interconnection support platforms.
- Stronger links between public sector and industry Cyber Hubs or SOCs. Promote cooperation and integration with the network of ISAC and other EU initiatives (e.g. CSIRT network and Cyber Hubs) toward a common and integrated situational awareness.
- Develop standardised approach to exchanging information and reporting/compliance[59]. Technical frameworks and mappings of taxonomies to allow for information exchange between Cross-Border Cyber Hubs.
- Develop and share trainings, including competitions such as Capture the Flag (CtF), on the basis of the ECSF, and exercises that would strengthen the cooperation among Cyber Hubs SOCs, ISACs and other EU initiatives and facilitate the sharing of information and notifications.
- Framework to facilitate the exchange[60] of best practices in setting up ISACs (focus on legal, information flows, operations, cybersecurity certification, etc.)

Type of action	Coordination and Support Action
Indicative budget	*2 mil EUR*-
Indicative call planning	2026
Indicative duration of the action	2-3 years
Implementation	ECCC

[59] information sharing formats and protocols, should be guided by and therefore take as their starting point guidelines issued by ENISA, according to Cyber Solidarity Act.

[60] Based on existing approaches already available, such as ENISA work on ISACS and information sharing: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing

Type of Beneficiaries	Cyber Hub operators
Security	Call for grants and procurement are restricted on the basis of Article 12(5) of the Regulation (EU) 2021/694.

2.10 Coordinated preparedness testing and other preparedness actions

This action covers two actions from the Cyber Solidarity Act, dedicated to Cybersecurity Emergency Mechanism, namely (1) coordinated preparedness testing of entities operating in sectors of high criticality across the Union and (2) other preparedness actions for entities operating in sectors of high criticality and other critical sectors.

2.10.1 Objective

These actions aim to complement and not duplicate efforts by Member States and those at Union level to increase the level of protection and resilience to cyber threats, in particular for critical industrial installations and infrastructures, by assisting Member States in their efforts to improve the preparedness for cyber threats and incidents by providing them with knowledge and expertise.

Proposals should contribute to achieving at least one of the objectives:

- (part 1) Coordinated preparedness testing of entities operating in sectors of high criticality across the Union (including penetration testing and threat assessment) considering ICT as well as Operational Technology/Industrial Control Systems.
- (part 2) Other preparedness actions for entities operating in sectors of high criticality and other critical sectors (i.e. vulnerability monitoring, exercises and trainings).

2.10.2 Scope

[Part 1 Coordinated preparedness testing]

The provision of preparedness support services shall include activities listed below, for entities in the sector or sub-sector as identified by the Commission in accordance with the Cyber Solidarity Act, from the Sectors of High Criticality listed in Annex I to Directive (EU) 2022/2555 and specified in the call for proposal document for each of the calls under this topic:

Support for testing for potential vulnerabilities:

- Development of **penetration testing** scenarios. The proposed scenarios may cover Networks, Applications, Virtualisation solutions, Cloud solutions, Industrial Control systems, and IoT.
- Support for conducting testing of essential entities operating critical infrastructure for potential vulnerabilities.

- Support the deployment of digital tools and infrastructures supporting the execution of testing scenarios and for conducting exercises such as the development of standardised cyber-ranges or other testing facilities, able to mimic features of critical sectors (e.g., energy sector, transport sector etc.) or others affected by NIS 2 to facilitate the execution of cyber-exercises, in particular within cross-border scenarios where relevant.
- Evaluation and/or testing of cybersecurity capabilities of MS entities and MS sectors (including capabilities to prevent, detect and respond to incidents and stress test of the entire sectors), evaluation and compliance activities aimed at increasing maturity e.g. on the basis of established maturity models and/or relevant evaluation and compliance schemes.
- Evaluation and/or testing of cybersecurity capabilities of entities in scope (including for the evaluation and management of risks concerning the supply chain).
- Consulting services, providing recommendations on how to improve infrastructure security and capabilities.

Support for **threat assessment and risk assessment**:

- Threat Assessment process implementation and life cycle
- Customised risk scenarios analysis.

The support will target relevant Member State competent authorities, which play a central role in the implementation of the NIS 2 Directive such as Computer Security Incident Response Teams (CSIRTs) and National Cybersecurity Authorities.

[Part 2 other preparedness actions]

For the second part, in addition to the services already listed for Part 1 (support for testing for potential vulnerabilities and support for threat assessment and risk management), the provision of preparedness support services included below, addressing entities operating in highly critical and other critical sectors as referred to in Annex I and II of the NIS2 Directive.

Support for **threat assessment and risk assessment**:

- Supply chain risk management within the risk assessment services.

Risk monitoring service:

- Specific continuous risk monitoring such as attack surface monitoring, risk monitoring of assets and vulnerabilities.

Support coordinated vulnerability disclosure and management:

- Promote the adoption of national CVD Policies[61] and the EU Vulnerability Database.

[61] Coordinated Vulnerability Disclosure Policies in the EU, ENISA, 2022, available at: https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-euassessment

- Coordinate the disclosure of vulnerabilities and timely dissemination of security patches. Standardisation of the way information is shared between different stakeholders in the vulnerability handling process.
- CVD applications that manage multiple sources of vulnerability information using open standards or technologies. (e.g. researchers, vendors, CSIRTs)
- Raise awareness on the adoption of vulnerability management best practices.

Dedicated exercises and trainings:

- Develop[62] comprehensive training programmes and workshops, including international ones, for cybersecurity professionals that will cover the latest trends in cyber threats, attack methodologies, and best practices for pre-threat management and prevention. Maturity checks, evaluation of cybersecurity capabilities.
- Encourage the development of cybersecurity life-long learning activities[63] to keep up with all cybersecurity requirements driven by EU cybersecurity related regulations and directives, including NIS 2 Directive, CSA, CSoA, DORA, EECC, GDPR, CRA.

The support will target relevant Member State competent authorities, which play a central role in the implementation of the NIS 2 Directive, Computer Security Incident Response Teams (CSIRTs) including sectorial CSIRTs, Security Operation Centres (SOC), highly critical and other critical sectors, industry stakeholders (including Information Sharing and Analysis Centres-ISACs) and any other actors within the scope of the NIS 2 Directive, DORA, CSA, etc.

Support may be provided amongst other for the on boarding to the CEF Cybersecurity Core Service Platforms of public and private organisations working on the implementation of the NIS 2 Directive and are potential users of the CEF Cybersecurity Core Service Platforms.

The action may also support industry, with a particular focus on start-ups and SMEs, to seize the industrial and market uptake opportunities created by the Cyber Resilience Act as well as support for the implementation of NIS 2 Directive.

2.10.3 Deliverables

The type of deliverables is also presented in two parts. First part covering:

- Enhanced cooperation, preparedness and cybersecurity resilience in the EU; preparedness support services
- Threat assessment and risk assessment services

For the second part, in addition:

- Risk monitoring services.
- Better compliance, coordinated vulnerability disclosure and monitoring.

[62] Based on the European Cybersecurity Skills Framework (ECSF)
[63] Based on ECSF

- Improved skills, via exercises and trainings, organization of events, workshops. stakeholder consultations and white papers.

For coordinated preparedness testing:

Type of action	Simple Grant
Indicative budget	*20 mil EUR (10 mil EUR in 2025 and 10 mil EUR in 2026)*
Indicative call planning	2025, 2026
Indicative duration of the action	3 years
Implementation	ECCC
Type of Beneficiaries	Public bodies acting as cybersecurity competent authorities or CSIRTs; Public bodies subject to NIS 2 directives, CRA, CSA, CSoA, DORA etc.
Security	Call for grants and procurement are restricted based on Article 12(5) of the Regulation (EU) 2021/694.

For other preparedness actions:

Type of action	Simple Grants
Indicative budget	*10 mil EUR (5 mil EUR in 2026 and 5 mil EUR in 2027)*
Indicative call planning	2026, 2027
Indicative duration of the action	3 years
Implementation	ECCC
Type of Beneficiaries	Public bodies acting as cybersecurity competent authorities or CSIRTs, national Cyber Hubs, as identified by Member States; Public bodies and other entities subject to NIS 2 directive (highly critical and other critical sectors entities), CRA, CSA, CSoA, DORA etc. Or[64] Industry stakeholders, other public and private entities that can support the implementation of NIS 2 directive (along to or for highly critical and other critical sectors entities), CRA, CSA, CSoA, DORA, GDPR, etc.
Security	Call for grants and procurement are restricted on the basis of Article 12(5) of the Regulation (EU) 2021/694.

2.11 Mutual assistance

[This will be reviewed after adoption of the Cyber Solidarity Act, as particular financial rules are introduced in the Act, not compliant with the current DEP regulation (i.e. retroactivity of costs). This action is delayed in this version to allow ECCC to prepare a methodology for the

[64] There should be separate calls for each type of beneficiaries.

implementation that will avoid any possible overlap with other activities financed by ECCC or ENISA.]

2.11.1 Objective

These actions aim to complement and not duplicate efforts by Member States and those at Union level to increase the capabilities to respond to the significant or large-scale cybersecurity incidents. In accordance with the Cyber Solidarity Act, it should provide support for technical assistance from one Member State to another Member State affected by a significant or large-scale cybersecurity incident, including in cases referred to in Article 11(3), point (f), of Directive (EU) 2022/2555.

2.11.2 Scope

The provision of mutual assistance support shall cover technical assistance of one Member State to another Member States to support responding to the significant or large-scale cybersecurity incidents. The technical assistance may include activities, as those listed below:

- Technical assistance with incident management.
- Information Security Incident Analysis and Crisis Communications as a retainer type of service.
- Artefact and Forensic Evidence collection and analysis preserving the chain of custody.
- Information Security Incident Coordination.
- Comprehensive reporting including scope, recommendations, remediation and findings.

The costs eligible to be covered by the support include dispatching of expert teams in the framework of mutual assistance. The eligible costs could include travel, accommodation and daily allowance expenses of cybersecurity experts.

The technical assistance can only be provided from one Member States cybersecurity competent authority, CSIRT to another Member State's cybersecurity competent authority, CSIRT and should be to support incident response activities for the significant or large-scale cybersecurity incident affecting entities operating in highly critical and other critical sectors defined in Directive (EU) 2022/2555.

The support shall be awarded directly without a call for proposals for grants[65].

In accordance with Article 193(2), second subparagraph, point (a), of Regulation (EU, Euratom) 2018/1046, in duly justified cases, the costs may be considered to be eligible even if they were incurred before the grant application was submitted.

In accordance with the Cyber Solidarity Act, by way of derogation from Article 12(1) of Regulation (EU, Euratom) 2018/1046, unused commitment and payment appropriations for

[65] A methodology will be developed before this activity will be implemented.

actions in the context of the implementation of the mutual assistance actions, shall be automatically carried over and may be committed and paid up to 31 December of the following financial year.

2.11.3 Deliverables

- Technical assistance in case of the significant and large-scale cybersecurity incident response.

Type of action	**Simple Grants (GRANT FOR NAMED BENEFICIARIES)**
Indicative budget	*4 mil EUR*
Indicative call planning	2026, 2027
Indicative duration of the action	3 years
Implementation	ECCC
Type of Beneficiaries	Public bodies acting as cybersecurity competent authority, CSIRTs designated or established pursuant to Article 10 of Directive (EU) 2022/2555
Security	Call for grants and procurement are restricted on the basis of Article 12(5) of the Regulation (EU) 2021/694.

Additional actions for improving EU cyber resilience

Several topics are presented in this section which are continuation of actions started in previous work programmes. All these actions are aimed at strengthening the cybersecurity posture of various stakeholders – NCCs, SMEs, start-ups, public and private bodies etc. that do have to comply with several legal requirements (i.e. Cyber Solidarity Act, Cyber Resilience, Act, DORA, Cybersecurity Act, NIS 2 Directive, GDPR, etc.) but do not fall in any of the previous categories.

2.12 Enhancing the NCC network

2.12.1 Objective

The National Coordination Centres (NCCs), set up by the Regulation (EU) 2021/887 are aimed to work together through a network and to contribute to achieving the objectives of the regulation and to foster the Cybersecurity Competence Community in each Member State, contributing to acquire the necessary capacity. National Coordination Centres can also support priority areas such as the implementation of EU legislation (Directive (EU) 2022/2555, the proposed Cyber Resilience Act and the Cybersecurity Act).

The objective of this topic is to support the operation of the NCCs and to enable them to support the cybersecurity community, including SMEs, for the uptake and dissemination of state-of-the-art cybersecurity solutions and strengthen cybersecurity capacities. Following financing received in previous years and different start date of operation in MSs, this activity aims to balance the resources available and to provide a similar financing to all NCCs.

This topic also considers providing support to the uptake of EU cybersecurity technologies and products, commercialisation and scale-up of European cybersecurity start-up/SME ecosystem, in collaboration and complementarity with the European 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, considering the use of public procurement and private investment direction.

An essential aspect of this action is to create a framework for the emergence of such incubators and accelerators in the Member States, based on best practices and considering the specific needs and requirements arising from EU legislation (such as the Cyber Resilience Act, NIS 2 directive).

In addition, this topic will contribute to the cybersecurity awareness. It is becoming increasingly important to inform and educate EU citizens to cybersecurity topics in their daily use of digital technologies. Cybersecurity awareness helps individuals and organisations to identify threats and take appropriate action. By promoting awareness, the likelihood of incidents and data breaches can be reduced. Within this topic, NCCs are encouraged to build upon ongoing initiatives, including for example the ones from the EC and ENISA, to improve the awareness of EU citizens, businesses and organisations on the cybersecurity risks and threats and to support cross European actions to increase the number of students studying cybersecurity; students engaged in cybersecurity research activities; students and young professionals choosing a career in cybersecurity.

Furthermore, European companies are innovative and develop highly competitive products, but the still underdeveloped Digital Single Market confines most of these companies (especially SMEs and start-ups) to their home country. A platform that opens the European market for small and medium-sized enterprises is also a springboard into international markets. This platform will ensure the competitiveness of European cybersecurity solutions. As such, this topic could also support the grow the EU Market for cybersecurity products and services by providing a platform on which European SMEs and start-ups can post their (market-ready) products and solutions and on which businesses, public authorities and private individuals can search for the best solution for their needs, regardless of the country.

2.12.2Scope

The National Coordination Centre should carry out, depending on their national context, one or more of the following tasks:

- acting as contact points at the national level for the Cybersecurity Competence Community to support the ECCC in achieving its objectives and missions.
- providing expertise and actively contributing to the strategic tasks of the ECCC, taking into account relevant national and regional challenges for cybersecurity in different sectors.
- promoting, encouraging and facilitating the participation of civil society, industry in particular start-ups and SMEs, academic and research communities and other actors

at Member State level in cross-border projects and cybersecurity actions funded through all relevant Union programmes.

- providing technical assistance to stakeholders by supporting the stakeholders in their application phase for projects managed by the ECCC, and in full compliance with the rules of sound financial management, especially on conflict of interests. This should be done in close coordination with relevant NCPs set up by Member States.
- seeking to establish synergies with relevant activities at national, regional and local levels, such as addressing cybersecurity in national policies on research, development and innovation in the area of, and in particular in those policies stated in the national cybersecurity strategies.
- Where relevant, implementing specific actions for which grants have been awarded by the ECCC, including through the provision of financial support to third parties in accordance with Article 204 of the Financial Regulation under conditions specified in the grant agreements concerned, in particular aimed at strengthening the uptake and dissemination of state-of-the-art cybersecurity solutions (notably by SMEs). Support scaling-up of start-ups by finding other funding for implementing existing projects.
- promoting and disseminating the relevant outcomes of the work of the Network and the ECCC at national, regional or local level.
- assessing requests for becoming part of the Cybersecurity Competence Community by entities established in the same Member State as the NCC.
- advocating and promoting involvement by relevant entities in the activities arising from the ECCC, the Network of National Coordination Centres, and the Cybersecurity Competence Community, and monitoring, as appropriate, the level of engagement with actions awarded for cybersecurity research, developments and deployments.
- Support the Cybersecurity Competence Community registration (on platforms such as ATLAS) and contribute to the development of suitable community management tools.

In addition, this action aims to promote safer digital behaviours, growth talents and attract more youth to cybersecurity careers, the NCCs could also, depending on their national context, carry out one or more of the following tasks:

- Provide support to innovative ideas towards market-readiness (for instance by launching a pan-European program where young individuals will be trained as ambassadors to promote cybersecurity awareness, best practices, and careers in schools, universities, and community events.)
- Strengthen collaboration between institutions for higher education, e.g. by jointly organizing events, by teaching students and working together on cutting-edge research. Support activities in primary and secondary levels of education to increase cybersecurity awareness and hygiene, through educating the teachers and educators.
- Build stronger partnerships with established SMEs, tech companies, and government agencies to develop and distribute software tools and services that assist in early threat detection, actor identification, and threat evolution monitoring. These

collaborations can ensure that cybersecurity professionals have access to the latest tools and technologies for effective threat management.

- Organise periodic cybersecurity boot camps, challenges, awareness campaigns and trainings across Europe, specifically for SMEs or students (e.g. focusing on equipping participants with hands-on skills to manage prevalent cyber threats through training sessions, workshops, and simulation activities tailored to their industry). Organise periodic awareness raising campaigns, at national and regional level, to increase cybersecurity awareness and hygiene aimed at different demographics. Organise national and regional cyber exercises to enhance the security and resilience of critical sectors as well as SMEs.
- Foster a community of cybersecurity professionals who can share their experiences, challenges, and solutions.
- Support and encourage the uptake of cybersecurity educational policy goals in national (cybersecurity) strategies.
- Promote safer digital behaviours and more youth considering cybersecurity careers.

The action could also aim to

- Support the adoption of market-ready innovative cybersecurity solutions, including solutions developed in the framework of EU-supported research and innovation projects.
- Provide and deploy up to date tools and services to organisations (in particular SMEs) to prepare, protect (e.g. network security, advanced two-factor or passwordless authentication) and respond to cybersecurity threats.

This topic targets exclusively National Coordination Centres which have been recognised by the Commission as having the capacity to manage funds to achieve the mission and objectives laid down in the Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. These actions aim at the operation of National Coordination Centres, which occupy a central role in the cybersecurity landscape as foreseen in Regulation (EU) 2021/887. Due to the synergetic role, they play with regards activities at national, regional and local levels, such as addressing cybersecurity in national policies on research, development and innovation in the area of, and in particular in those policies stated in the national cybersecurity strategies, they must be able to handle sensitive information, and be protected against possible dependencies and vulnerabilities in cybersecurity to pre-empt undue foreign influence and control.

As previously noted, participation of non-EU entities entails the risk of highly sensitive information about security infrastructure, risks and incidents being subject to legislation or pressure that obliges those non-EU entities to disclose this information to non-EU governments, with an unpredictable security risk. Therefore, based on the outlined security reasons, the actions are subject to Article 12(5) of Regulation (EU) 2021/694.

2.12.3 Outcomes and deliverables

One or more of the following should be covered:

- Network of national initiatives aimed to accelerate the cybersecurity industry and facilitate the access-to-market.
- European frameworks for establishing cybersecurity incubators and accelerators.
- Cybersecurity Community Observatory to inform subsequent policy interventions by the ECCC and NCCs.
- Matchmaking events to create connections and build trust; platforms and events for Access-to-Finance and Access-to-Market.
- Strengthened Cybersecurity Community to support the European Cybersecurity Industrial, Technology and Research Competence Centre.
- Uptake of cybersecurity solutions.
- Strengthened cybersecurity capacities of stakeholders.
- Synergetic activities that strengthen the role of NCC.
- Centralize the many initiatives focusing on raising awareness and work together with other NCCs to support a cross European approach covering education, studies, trainings and awareness campaigns[66] ; Share and provide best practices related to the awareness topic.
- Support the transfer of best practices related to cybersecurity teaching for primary and secondary school and other activities for children and youngsters (including camps, materials, games, etc.). Support for teachers and professors to have access to best practices available in the EU and facilitate their dialog.
- Cyber campaign material focused on young professionals and students of all ages and gender to pursue and advance in cybersecurity careers, where the NCCs can build on in view of regional differences.
- Cyber campaign material focused on parents and teachers of future students of all ages and gender to raise the number of cybersecurity students.
- Platform supporting a network of young cybersecurity ambassadors spreading awareness and fostering a culture of cybersecurity among Europe's youth.
- Common services to be provided within national cyber campuses.
- Hybrid events for the cybersecurity competence community to increase awareness of cybersecurity threats, threat actor modus operandi and potential impact, potentially in collaboration with existing initiatives and platforms.

In addition, activities could cover, the set up a platform integrating all other existing platforms, hosted and maintained at the European level under the .eu domain, so as to:

[66] The activities should consider other ongoing projects, activities, campaigns as well as the mandate of ENISA and other EU or national bodies. These actions should ensure synergies at EU level and should not duplicate efforts at EU or national levels.

- Establish and maintain a marketplace for cybersecurity products and services.
- Allowing to retrieve information on entities adhering to the 27 NCC communities.

Type of action	Simple grant
Indicative budget	*35 mil EUR*
Indicative call planning	2026
Indicative duration of the action	3-4 years
Implementation	ECCC
Type of Beneficiaries	National Coordination Centres and other private and public entities in consortium with NCCs, including academia and research entities.
Security	Call restricted on the basis of Article 12(5) of the Digital Europe Programme Regulation (EU) 2021/694.

2.13 Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements

2.13.1 Objective

The objective of this topic is to support European ecosystem to strengthen their cybersecurity capacities and to support the implementation of the regulatory framework in line with Cyber Resilience Act (CRA), NIS 2 Directive, GDPR, DORA, Cybersecurity Act, etc. in a homogeneous approach. Additionally, and in alignment with the Digital education plan, which emphasizes the development of digital skills crucial for the modern economy, and in support of initiatives like the Cybersecurity Skills Academy, activities related to cybersecurity challenges should also be promoted. These initiatives aim to address the skills shortage in cybersecurity and develop a workforce capable of meeting regulatory and operational demands. By providing practical training, attracting young professionals, and encouraging diversity within the field, these efforts are vital to Europe's ability to respond to evolving cyber threats and comply with new legislation. Additionally, these activities foster equal opportunities and raise cybersecurity awareness among future generations, contributing to Europe's broader strategic goals in the digital domain.

The implementation of EU cybersecurity legislation needs to be supported to achieve a higher level of cybersecurity in the EU, especially in a constantly changing threat landscape. Cybersecurity maturity levels are different in sectors. This means that efforts and investments are needed to ensure and continuously improve cyber security in both the public and private sectors. Such efforts and investments are crucial in each Member State and therefore require increased focus and joint efforts at European level. Empowerment and self-assessment tools can be the most effective.

All the above efforts should consider that security and protection of data must be promoted during the design and development of ICT products and services.

2.13.2 Scope

EU cybersecurity legislation brings new responsibilities and imposes obligations on key stakeholders, ICT systems, Operational Technology and IoT manufacturers. For instance, the cost of obtaining a cybersecurity certification for an ICT or digital product, service or process is often an insuperable barrier for EU start-ups and SMEs.

Support must be provided for the implementation of these obligations. The activities under this action require various types of support, including financial and organisational.

The focus will also be on fostering cross-border collaboration and promoting diversity within the cybersecurity workforce, encouraging participation from women and other underrepresented groups. In conjunction with initiatives like the Cybersecurity Skills Academy, these activities will contribute to building capacity, raising awareness, and supporting the uptake of the aforementioned regulatory framework. By integrating these challenges into a broader capacity-building framework, they will ensure that stakeholders across sectors are equipped to address evolving cybersecurity threats and comply with the new legislative landscape.

Aligned with the goals of the Digital Education Action Plan which focuses on enhancing digital skills across Europe, activities related to cybersecurity challenges will play a crucial role in developing the next generation of cybersecurity professionals. These challenges will provide hands-on experience for young professionals and students, helping to close the cybersecurity skills gap and ensuring they are well-prepared to meet the demands of new legislative requirements.

The assessment of products and services is an essential step in the EU cybersecurity certification process. As cybersecurity threats are rapidly evolving and attacks are becoming more sophisticated, it is important to find a way to address these challenges. In addition, the EU needs to cope with the continuous growth of information systems (in terms of size and complexity) and the significant expansion of the digital space by enabling fast but secure replication of assessments. Furthermore, it is a great opportunity for the EU to develop interoperable solutions that will increase its competitiveness. In doing so, the Union can rely on a large and dynamic number of players who have already developed high-quality offerings.

The certification process is also very formal in terms of the documentation that is later used as proof for issuing the certificate. There is currently no platform to help proponents overcome the challenges posed by the use of many different and complex documents by all parties.

This action involves building capacity of national cybersecurity certification authorities to undertake market surveillance and supervise conformity assessment bodies and conformity assessments of essential requirements for cybersecurity products, services and processes. It should ensure the mutual recognition across Member States.

Furthermore, the action is also about building up capabilities of conformity assessment bodies and certification laboratories to meet the requirements of the Cyber Security Act and the

Cyber Resilience Act, as regards verifying declarations of conformity from suppliers and vendors.

The action involves also the development of supporting tools for certification and evaluation processes, including a "Certification and Evaluation as a Service" software platform to assist conformity assessment as well as supporting in creating national or cross-regional expert hubs to assist with these processes. Its development should involve relevant stakeholders such as CB's, CABs', and client representatives.

The "Certification and Evaluation as a Service platform" could facilitate and streamline the management of all documentation used in the certification process. It could also help to speed up the information exchange between the bodies taking part in the process. The platform could help to harmonize and standardise the documentation and tools to be used in whole Europe.

The main areas considered under the scope of this action could include:

- The implementation of EU legislation in cybersecurity to be supported to achieve a higher cybersecurity level in Europe.
- Provide support to SMEs aiming to enhance cybersecurity resilience with a particular focus on legal requirements deriving from EU legislation such as NIS 2, Cyber Resilience Act, Cybersecurity Act etc. including practical guidelines and user-friendly tools allowing the company to check whether its solutions are compliant with the requirements of the new legislation considering open standards.
- Develop reporting platforms for NIS2 (e.g. incident reporting platform) and CRA (e.g. vulnerability single reporting platform).
- Establish short-term and long-term actions aimed at preparing the professionals to implement properly the requirements of new EU regulations in entities covered by those regulations.
- Develop programs to promote diversity and equal opportunities for all young Europeans, providing tailored onboarding programs for youth. These programs will offer resources and easy access to educational content, ensuring that participants from various backgrounds can engage with cybersecurity training. By supporting non-formal education and offering participation opportunities, such as cybersecurity challenges, these efforts will help equip the next generation with the skills needed to thrive in the sector.
- Creation and development of cooperation initiatives in cross-border and cross-sector contexts. Encourage collaboration between national authorities to enhance cyber resilience and raise cybersecurity maturity levels through development and implementation of common methodologies.
- Design and evaluation of platforms for training programs and tools for cross-country exchange will support these efforts. Additionally, benchmarking and assessment programs will help optimize performance, enhancing participants' skills. These initiatives, including training materials, with cybersecurity challenges as one example,

will also include peer exchange and fellowship opportunities, fostering a connected community of cybersecurity professionals. By encouraging cross-border collaboration and ongoing engagement, these programs aim to strengthen Europe's cybersecurity workforce and support long-term talent development.

- Support the development of cross-border collaboration programs, enabling pan-European teams to participate in international cybersecurity competitions, enhancing visibility and competitiveness on the global stage. These initiatives will provide teams with access to advanced tools, mentorship, and leadership training, fostering the growth of a European cybersecurity talent pipeline. By promoting excellence, skills development, and leadership, this support will ensure that Europe's top talent remains competitive, well-prepared, and collaborative in facing global cybersecurity challenges.

In addition to providing supports for national cybersecurity certification authorities, conformity assessment bodies and national accreditation bodies with certification, the implementation of the NIS 2 Directive will continue in the coming years. In particular, competent authorities will need to build up capacity in audit and compliance to ensure that essential and important entities are meeting their responsibilities. Training and awareness raising activities along with trust and confidence building activities to ease information sharing and knowledge building should be provisioned.

Overall, this action is intended to increase collaboration between national authorities, supporting or supplementing the structures under the NIS Directive and that need to comply with CRA (e.g. Software Bill of Materials, CRA Single Reporting Platform contributions and open prototypes, CVD processes or security advisory automation, like the CSAF), as well as between national authorities and stakeholders, especially SMEs, to raise cybersecurity maturity levels through the development and implementation of common methodologies to enable deployment of cybersecurity processes and the uptake of products and services by entities.

This action involves creation, and deployment of common tools for regulation and enforcement, including targeted security audits, incident notifications to national competent authorities and for ease of information exchange.

Under information exchange, the action can also include:

- At national level, federate national actors working on cyber threat intelligence and national competent authorities around a common platform. Including easing and centralising the notification process for NIS 2 entities.
- At vertical level within the EU, organize or support cyber threats intelligence (CTI) unclassified information sharing in confidence between stakeholders of the given vertical.
- At EU level, enabling and organizing countries collaboration and information sharing.
- Collaborate on and enrol a framework of guidelines - in the EU or multiple EU MS - to ensure and continuously improve cybersecurity both within the public and private

sectors through better protection of their data, a significant reduction of the risk of the most common cyberattacks, and an increase of cyber resilience in general.

In addition, this topic promotes security and privacy 'by design' in existing and emerging technologies, applications and hardware, including IoT, Operational Technology, -Identity and e-government systems, by supporting and/or funding research and innovation opportunities. Privacy-enhancing technologies aim to minimise the risks to the privacy of data subjects. Implementing security and privacy features in emerging technologies, applications and hardware from the outset - in the design and implementation phase[67] - ensures that potential vulnerabilities and risks are recognised and addressed early in the development process. In addition, to be in line with data protection regulations, this approach can be more cost-effective and would reduce the likelihood of security and personal data breaches.

Consortia should consider including at least one representative of each of the following categories to reflect the whole value chain: privacy enhancing technologies researchers, privacy enhancing technology providers, ICT product and services developers, which integrate privacy enhancing technologies, and ICT product and services user organizations.

2.13.3 Deliverables

One or more of the following should be covered:

- Implementation of guidelines, standardised processes, or manuals - in the EU or multiple EU MS concerning the most challenging issues, supporting specific stakeholders and sectors addressed by cybersecurity legislation.
- Develop and implement tools, raise awareness and encourage and facilitate industry uptake, with a focus on SMEs, of conformity assessments of essential cybersecurity requirements for products with digital elements (hardware and software) under the CRA.
- Support for mechanisms reducing administrative burden for entities, like single entry point for incident notification.
- Establish secure communication channels allowing for cooperation and information sharing initiatives.
- Support organization of regular meetings/workshops to identify good practices within specific sectors or emerging areas and also facilitate collaborative efforts between different sectors
- Support development of trainings, on the basis of the ECSF and exercises that promote capacity building and internal awareness.

[67] Data Protection Engineering, ENISA, 2022, available at https://www.enisa.europa.eu/publications/data-protection-engineering

- **Contribution to CR standardisation**: Training materials and training actions on cybersecurity certification for national authorities and conformity assessment bodies.
- **Certification Fostering:** Educative and supportive materials and an explanatory press campaign using interactive material such as “do I comply with CRA”. Information campaign through various channels such as conferences, meetings, etc. Website dedicated to the mandatory certification and conformity assessments of essential requirements.
- Development of training programs and material(s), including tools for cross-country collaboration and exchange, aimed at enhancing participants' skills and readiness for real-world threats. These programs can also support non-formal education for high school students and teachers, enhancing digital literacy and cybersecurity awareness at early educational levels.
- Creation of benchmarking and assessment programs to evaluate and optimize the performance of participants in cybersecurity training programs, ensuring continuous improvement and alignment with industry standards.
- Implement peer exchange and fellowship programs, aimed at fostering a connected, resilient community of cybersecurity professionals across Europe. These programs will also include support for cross-border training initiatives and non-formal education activities, ensuring that both students and educators can participate in hands-on cybersecurity learning experiences and contribute to long-term talent development
- Establishment of cross-border collaboration programs to support the development of pan-European teams in cybersecurity competitions. These programs will provide access to mentorship, advanced tools, and leadership training, ensuring European teams remain competitive on the global stage. Additionally, the programs will foster the growth of a European cybersecurity leadership pipeline, enhancing Europe's visibility and effectiveness in international cybersecurity challenges.
- Support organizations, including SMEs, to assess the robustness, applicability and relevance of security and privacy enhancing technologies for their integration to the ICT products and services they develop.
- Set-up pilot projects to test CRA compliance, use open-source software and libraries for conformity assessment and testing; develop methodologies for assessment for the purpose of CRA compliance/requirements.
- Develop best practices or guidelines for setting-up and functioning of market surveillance authorities of MSs; develop awareness of CRA requirements.
- Support organizations, including SMEs, to stimulate commercialization of privacy enhancing technologies and demonstrate how they can address security and privacy risks from emerging technologies.
- Facilitate cooperation between the producers of emerging technologies, the users of those technologies and regulators. Such cooperation would allow to identify which requirements can be met by which privacy enhancing technology, in which use cases,

to what extent they could facilitate compliance or reduce the cost thereof, and how to engineer it in practice, during the early phases of design and development of ICT products and services.

- Strengthen the cooperation among the whole value chain of between privacy enhancing technology including researchers, providers, integrators and users, and GDPR national authorities/European supervisors.

Type of action	Simple grant
Indicative budget	*31 mil EUR*
Indicative call planning	2026, 2027
Indicative duration of the action	3 years
Implementation	ECCC
Type of Beneficiaries	All stakeholders
Security	Call restricted on the basis of Article 12(5) of the Digital Europe Programme Regulation (EU) 2021/694.

2.14 Dedicated action to reinforcing hospitals and healthcare providers

2.14.1 Objective:

This action aims to help strengthen the cybersecurity defenses of hospitals and healthcare providers. The goal is to ensure that hospitals and healthcare providers, which are crucial operators in the health sector, can effectively detect, monitor, and respond to cyber threats, particularly ransomware, which pose significant risks thereby enhancing the resilience of the European healthcare system.

The action will contribute to the forthcoming EU action plan on cybersecurity in hospitals and healthcare.

2.14.2 Scope

This action addresses the growing need for continuous cybersecurity monitoring, threat intelligence, and incident response in hospitals and healthcare providers, which often lack dedicated cybersecurity resources for adequately protecting themselves from cyber threats.

The action will support pilot projects, which will bring together stakeholders such as regional and/or national clusters associations[68] of hospitals and healthcare providers (such as national healthcare systems, hospitals or associations of hospitals, healthcare providers and/or

[68] 'Cluster associations' refers to any legally established group of hospitals and healthcare providers such as, for examples, regions and professional associations established in one or more Member States.

professional associations of healthcare practitioners), as well as cybersecurity service providers.

The pilot projects will define the state of preparedness of clusters of hospitals and healthcare providers in the European Union, to be able to assess their needs. Based on this analysis, they will prepare an overview of the state-of-the-art cybersecurity solutions and resources needed (technologies, services, tools, human resources, training needs, etc.) for hospitals and healthcare providers to meet the scope of the action. These may include for example: Security Operation Centres services that offer real-time monitoring, threat detection, and rapid incident response, and advanced cybersecurity tools, such as Security Information and Event Management (SIEM) platforms, threat intelligence, and automated response capabilities or other.

The pilots will develop technical plans, tailored to the needs of representative hospitals and healthcare providers (e.g., small or large hospitals, private healthcare providers, etc.) which will also need to include best implementation recommendations and cost estimates for effective deployment.

The pilot projects will conduct a demo implementation of these technical plans to demonstrate their effectiveness in operations at the stakeholders' sites, showcasing different use cases for different user groups at small, medium and large hospitals and healthcare providers, at least in two different Member States.

The pilot projects will serve as demonstration projects and will also provide cybersecurity education and training to the staff of their partner hospitals and healthcare providers, enhancing awareness and ensuring best practices in safeguarding sensitive healthcare information.

Finally, in cooperation with each other, the pilot projects will undertake wide dissemination activities of best practices across the EU, with the specific goal of helping replicate and scale up the pilots activities as widely as possible.

The pilot projects will support healthcare institutions complying with the NIS2 directive.

2.14.3 Deliverables

- Mapping of common cybersecurity needs of hospitals and healthcare providers.
- Guidelines for healthcare providers to assess their current state of cybersecurity protection and relevant needs.
- Technical cybersecurity plans to enhance preparedness and cyber resilience: improved detection and response capabilities for healthcare institutions minimizing the impact of cyber-attacks, particularly for ransomware. This also includes dedicated trainings to staff.
- Pilot cybersecurity demo installations at partner hospitals and healthcare providers sites to ensure hospitals and healthcare providers can maintain operational continuity in the face of cybersecurity incidents. This should be monitored through specific KPIs.

- Wide dissemination campaigns to help scale up preparedness of hospitals and healthcare providers in Europe.

2.14.4 Consortia eligibility

Consortia shall include regional and/or national clusters of hospitals and healthcare providers from at least two EU Member States (such as national healthcare systems, hospitals or associations of hospitals, healthcare providers and/or professional associations of healthcare practitioners), comprising small, medium and large size entities, as well as cybersecurity service providers.

Type of action	Simple grant
Indicative budget	*30 mil EUR*
Indicative call planning	2025
Indicative duration of the action	1,5-2 years
Implementation	ECCC
Type of Beneficiaries	Private and public entities
Security	Call restricted on the basis of Article 12(5) of the Digital Europe Programme Regulation (EU) 2021/694.

2.15 Dual use technologies

2.15.1 Objectives

The objective is to enhance cooperation between the civil and defence spheres regarding dual-use projects, services, competences and applications in cybersecurity in line with the DEP Regulation, Article 6.1 (f) and ECCC Regulation, Article 5.3(g).

This should foster synergies between cybersecurity actions in Horizon Europe, Digital Europe and defence related actions carried out by the Union through its bodies and programmes, such as the European Defence Agency and the European Defence Fund (EDF).

Since the beginning of DEP, this objective had limited coverage and only one call[69] was launched in 2023.

2.15.2 Scope

The objective is to enhance cooperation between the civil and defence spheres through the development of dual use working prototypes, ready to the market products and operational infrastructures related to cybersecurity technologies, applications and tools that have

[69] DIGITAL-ECCC-2023-DEPLOY-CYBER-04-CIVIL-DEFENCE

relevance in both civilian and defence context. Examples of interest domains for this call topic are:

- AI empowered cybersecurity early warning, situation awareness and detection systems.
- GDPR compliant cybersurveillance and monitoring systems.
- Post quantum based secure communication systems.
- Survivable networks paradigms.
- AI driven cyberthreats mitigation and recovery systems.
- Securing unmanned vehicles (underwater and aerial vehicles).

Other cybersecurity domains where civil and defence spheres have a common interest to develop working systems together will also fall within the boundaries of this call topic.

Products and/or services will be further detailed in white papers during the implementation of the project.

Upon ECCC request, project consortia will participate to clustering activities to define common actions and for enhancing the synergies between the civil and defence communities.

2.15.3 Deliverables

- Development of dual use cybersecurity working prototypes and ready to the market products.
- Development of Dual-use Cybersecurity infrastructures and tools.
- Development Dual-use cybersecurity technologies proof-of-concept supported by a working prototype.
- Dual-use cyber-security dataset and data-lakes.
- Deployment of cybersecurity AI algorithms and techniques supported by a working prototype.
- White papers for products and/or services common to the cybersecurity civilian and defence spheres.
- Synergies between these communities, such as common activities to define common actions.

Type of action	Simple grants
Indicative budget	*10 mil EUR*
Indicative call planning	2026
Indicative duration of the action	3 years
Implementation	ECCC
Type of Beneficiaries	Stakeholders in either Cybersecurity Civilian and Defence Sphere, aiming at fostering joint collaborations targeting the delivery of

	concrete systems, tools and technologies, such as industrial players, Defence Ministries and Agencies, SMEs and start-ups and relevant actors that play a role in the European Cybersecurity Civilian and Defence Spheres. Multi-country consortia composition is not mandatory for this topic but will positively contribute to the impact of the action.
Security	Call restricted on the basis of Article 12(5) of the Digital Europe Programme Regulation (EU) 2021/694.

3 Programme Support Actions

Programme support actions with a budget of EUR 9 million aim at maximising the impact of the EU intervention while avoiding duplication and maximizing synergies with ongoing activities performed at national or EU level. Horizontal actions will cover costs including preparation, evaluation, monitoring and studies. An amount of funding will be set aside to cover awareness and dissemination as it is crucial to effectively communicate about the value and benefits of the Digital Europe Programme. As an indicative list, programme support actions funded under this Work Programme might cover:

1. External expertise:
    - The use of appointed independent experts for the evaluation of the project proposals and where appropriate, the monitoring of running projects.
    - The use of individual independent experts to advise on, or support, the design and implementation of the underpinning policy.

2. Studies and other support actions related to DEP and DEP implementation:
    - Events (including presidency events).
    - Support to community engagement and building.
    - Support to enhance gender balance in cybersecurity.
    - Publications.
    - Communication.
    - Studies, including mapping exercise foreseen by Cyber Solidarity Act.
    - Other support measures, e.g. support to the Cyber Security Atlas.

4 Implementation

The programme counts with two main implementation modes: procurement and grants.

The different nature and specificities of the actions indicated in the previous chapters require distinctive implementation measures. Each of these will therefore be achieved through various implementation modes.

Proposers are strongly encouraged to follow green public procurement principles and take account of life cycle costs[70].

The implementation is articulated through different types of actions, which are indicated in each topic. More details on each type of action are described in Appendix 2.

[70] http://ec.europa.eu/environment/gpp/index_en.htm (Oct. 6, 2021)

4.1 Procurement

Procurement actions will be carried out in compliance with the applicable EU public procurement rules. The procedures will be implemented either through direct calls for tenders or by using existing framework contracts. IT development and procurement activities will be carried out in compliance with European Commission's applicable IT governance rules[71].

4.2 Grants – Calls for Proposals

4.2.1 Evaluation Process

The evaluation of proposals will be based on the principles of transparency and equal treatment. It will be carried out by the ECCC[72] and with the assistance of independent experts.

4.2.1.1 Admissibility conditions

Proposals must be submitted before the call deadline and only through the means specified in the call for proposals. The call deadline is a deadline for receipt of proposals.

Proposals must be complete and contain all parts and mandatory annexes and supporting documents specified in the call for proposals. Incomplete proposals may be considered inadmissible.

4.2.1.2 Eligibility criteria

Proposals will be eligible if they are submitted by entities and/or consortiums compliant with the requirements set out in this Work Programme and the relevant call for proposals. Only proposals meeting the requirements of the eligibility criteria in the call for proposals will be evaluated further.

4.2.1.3 Exclusion criteria

Applicants which are subject to EU administrative sanctions (i.e. exclusion or financial penalty decision)[73] might be excluded from participation. Specific exclusion criteria will be listed in the call for proposals.

4.2.1.4 Financial and operational capacity

Each individual applicant must have stable and sufficient resources as well as the know-how and qualification to successfully implement the projects and contribute their share. Organisations participating in several projects must have sufficient capacity to implement all

[71] To be checked if pre-approval by European Commission Information and Cybersecurity Board is needed or some compliance with new EU bodies regulation for cybersecurity.
[72] ECCC together with the Commission services if needed.
[73] See article 136 of EU Financial Regulation 2018/1046.

these projects. Applicants must demonstrate their financial and operational capacity to carry out the proposed action.

4.2.1.5 Award criteria

The three sets of criteria are listed in Appendix 1 of this Work Programme. Each of the eligible proposals will be evaluated against the award criteria. Proposals responding to a specific topic as defined in the previous chapters of this Work Programme will be evaluated both individually and comparatively. The comparative assessment of proposals will cover all proposals responding to the same topic.

Proposals that achieve a score greater than or equal to the threshold will be ranked within the objective. These rankings will determine the order of priority for funding. Following evaluation of award criteria, the Commission establishes a Selection Decision taking into account the scores and ranking of the proposals, the programme priorities and the available budget.

The coordinators of all submitted proposals will be informed in writing about the outcome of the evaluation for their proposal(s).

4.2.2 Selection of Independent Experts for Evaluation and Reviews

The Commission and the Executive Agency will select independent experts to assist with the evaluation of proposals and with the review of project results as well as for other purposes where specific expertise might be required for implementation of the Programme. Experts are invited to apply using the mechanisms and tools provided for in the Horizon Programme[74] and a list of experts appropriate to the requirements of the Digital Europe Programme and each addressed area will be established. Experts will be selected from this list on the basis of their ability to perform the tasks assigned to them, taking into account the thematic requirements of the topic, and with consideration of geographical and gender balance as well as the requirement to prevent and manage (potential) conflicts of interest.

4.2.3 Indicative Implementation Calendar

The indicative calendar for the implementation of the Digital Europe calls for proposals in the context of this Work Programme foresees one call, during Q1, each year, covering all topics identified for the specific year. (Deadline for submission to be set in Q3 and evaluation to take place in Q1 the following year, with an aim to have all contact signed by Q3 following year.) This planning does not prevent the opening of additional calls if needed.

More information about these calls will be available on: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home.

[74] http://ec.europa.eu/research/participants/portal/desktop/en/experts/index.html

5 Appendices

Appendix 1 – Award Criteria for the Calls for Proposals

Proposals are evaluated and scored against award criteria set out for each topic in the call document. The general award criteria for the Digital Europe calls are as follows:

1. Relevance:

- Alignment with the objectives and activities as described in the call for proposals.
- Contribution to long-term policy objectives, relevant policies and strategies, and synergies with activities at European and national level.
- Extent to which the project would reinforce and secure the digital technology supply chain in the EU*.
- Extent to which the project can overcome financial obstacles such as the lack of market finance*.

* This might not be applicable to all topics

2. Implementation

- Maturity of the project.
- Soundness of the implementation plan and efficient use of resources.
- Capacity of the applicants, and when applicable the consortium as a whole, to carry out the proposed work.

3. Impact

- Extent to which the project will achieve the expected outcomes and deliverables referred to in the call for proposals and, when relevant, the plans to disseminate and communicate project achievements.
- Extent to which the project will strengthen competitiveness and bring important benefits for society.
- Extent to which the project addresses environmental sustainability and the European Green Deal goals, in terms of direct effects and/or in awareness of environmental effects*.

*This might not be applicable to all topics and in only exceptional occasions and for duly justified reasons may not be evaluated (see specific topic conditions in the call for proposals).

Appendix 2 – Types of action to be implemented through grants

The descriptions below of the types of actions to be implemented through grants under the Digital Europe Programme is indicative and should help the (potential) applicants to

understand the expectation in each type of action. The call text will define the objectives and scope of the action in more detail.

Simple Grants

Description: The simple grants are a flexible type of action used by a large variety of topics and can cover most activities. The consortium will mostly use personnel costs to implement action tasks, activities with third parties (subcontracting, financial support, purchase) are possible but should be limited.

Funding rate: 50% of total eligible costs for all beneficiaries.

SME support actions

Description: Type of action primarily consisting of activities directly aiming at supporting SMEs involved in building up and the deployment of the digital capacities. This action can also be used if SME needs to be in the consortium and make investments to access the digital capacities.

Funding rate: 50% of total eligible costs except for SMEs where a rate of 75% applies.

Coordination and support actions (CSA):

Description: Small type of action with the primary goal to promote cooperation and/or promote support to EU policies. Activities can include coordination between different actors for accompanying measures such as standardisation, dissemination, awareness-raising and communication, networking, coordination or support services, policy dialogues and mutual learning exercises and studies, including design studies for new infrastructure. CSA may also include complementary activities of strategic planning, networking and coordination between programmes in different countries.

Funding rate: 100% of eligible costs.

Grant for financial support

Description: Actions with a particular focus on providing financial support to third parties. The majority of the grant will be distributed via financial support to third parties with special provisions in the grant agreement, maximum amounts to third parties, multiple pre-financing and reporting obligations.

Annex 5 of the model grant agreements foresees specific rules for this type of action regarding conflict of interest, the principles of transparency, non-discrimination and sound financial management as well as the selection procedure and criteria.

In order to assure the co-financing obligation in the programme, the support to third parties should only cover 50% of third-party costs.

Funding rate: 100% of eligible costs for the consortium, co-financing of 50% of total eligible costs by the supported third party.

Appendix 3- Implementation of Article 12(5) Regulation (EU) 2021/694

As indicated in this document, as will be additionally detailed in the call document, and if justified for security reasons, an action falling under Specific Objective 3 can exclude the participation of legal entities controlled by a third country[75] (including those established in the EU territory but controlled by a third country or by a third country legal entity). EEA EFTA countries are fully associated to the Digital Europe Programme and benefit from a status equivalent to that of the Member States.

The assessment of the foreign control is part of the eligibility criteria. For this purpose, participants will be requested to fill in a self-assessment questionnaire to determine their control status during proposal submission. They will also be requested to submit supporting documents in order for the Commission to determine that the entities are not controlled by a third country.

More information will be published in the Funding and Tenders portal and in the procurement-related documents.

In the particular case of section 2.1 (Cyber Hubs), exceptionally, when in order to fulfil the objectives of the Cyber Solidarity Act, it is necessary, for duly justified reasons, to procure the provision of subscription services for information aiming to enhance cybersecurity situational awareness, the procuring authority may allow legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States to use as subcontractors, suppliers established in or controlled by third countries, subject to strict security conditions, in order to ensure sufficient diversity and geographical coverage of the information in the subscription services procured.

Where the contracting authorities allow the use of subcontractors who are suppliers that are not EU-controlled, the tendering documents shall set out that the services (or components thereof) shall fulfil requirements that guarantee the protection of the essential security interests of the Union and the Member States and ensure the protection of classified information. Such security conditions must be objective, non-discriminatory and must be duly justified under Union law, including in accordance with the exceptions foreseen in the relevant international agreements.

[75] See article 12(5) of the Digital Europe Programme Regulation

Appendix 4: Restrictions for the protection of European digital infrastructures, communication and information systems, and related supply chains

The protection of European communication networks has been identified as an important security interest of the Union and its Member States[76]. In line with the Commission Recommendation on the cybersecurity of 5G networks of 2019[77] and the subsequent report on EU coordinated risk assessment of the cybersecurity of 5G networks of 2019[78], the EU Toolbox on 5G cybersecurity[79], the second report on Member States' progress in implementing the EU toolbox on 5G cybersecurity of 2023[80], and the related Communication on the implementation of the 5G cybersecurity toolbox of 2023[81], the Commission together with the Member States has worked to jointly identify and assess cyberthreats and security risks for 5G networks[82]. The toolbox also recommends adding country-specific information (e.g. threat assessment from national security services, etc.). This work is an essential component of the Security Union Strategy and supports the protection of electronic communications networks and other critical infrastructures.

Entities assessed as "high-risk suppliers", are currently set out in the second report on Member States' progress in implementing the EU toolbox on 5G cybersecurity of 2023[83] and the related Communication on the implementation of the 5G cybersecurity toolbox of 2023[84].

In accordance with Article 136(2) of the Financial Regulation[85], this Work Programme has identified actions that concern strategic assets and interests of the Union or its Member States, for which it sets out specific award procedures aimed at ensuring the protection of

[76] European Council conclusions of 1 and 2 October 2020 (EUCO 13/20), point 11; Council Conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G, 14517/19.
[77] Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks, L 88/42.
[78] NIS Cooperation Group, Report on EU coordinated risk assessment of the cybersecurity of 5G networks, 9 October 2019.
[79] NIS Cooperation Group, EU Toolbox on 5G Cybersecurity, 29 January 2020.
[80] NIS Cooperation Group, Second report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity, June 2023.
[81] Communication from the Commission: Implementation of the 5g cybersecurity Toolbox, Brussels, 15.6.2023 C(2023) 4049 final.
[82] Within the NIS framework NIS 1 + 2 [Directive - 2022/2555 - EN - EUR-Lex (europa.eu)]
[83] NIS Cooperation Group, Second report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity, June 2023.
[84] Communication from the Commission: Implementation of the 5G cybersecurity Toolbox, Brussels, 15.6.2023 C(2023) 4049 final
[85] Regulation (EU, Euratom) 2024/2509 of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union

the integrity of digital infrastructure, communication and information systems, and related supply chains.

This entails the need to avoid the participation of high-risk supplier entities and the use of non-secure equipment and other goods, works and/or services in the deployment of key digital infrastructures, communication and information systems, and related supply chains to prevent technology transfer and the persistence of dependencies in materials, semiconductor components (including processors), computing resources, software tools and virtualisation technologies, and to preserve the integrity of the concerned systems, including from a cybersecurity perspective.

In order to protect the concerned strategic assets and interests of the Union or its Member States, it is therefore appropriate that the two following additional eligibility criteria apply to the actions listed below and identified in the WP as "subject to restrictions for the protection of European digital infrastructures, communication and information systems, and related supply chains":

1. Entities that are assessed as high-risk suppliers of mobile network communication equipment (and any entities they own or control) are not eligible to participate in any capacity, including as beneficiaries, affiliated entities, associated partners, third parties giving in-kind contributions, subcontractors or recipients of financial support to third parties (if any).

The assessment is based on the following criteria:

- likelihood of interference from a non-associated third country, for example due to:
  - the characteristics of the entity's ownership or governance (e.g. state-owned or controlled, government/party involvement).
  - the characteristics of the entity's business and other conduct (e.g. a strong link to a third country government).
  - the characteristics of the respective third country (e.g. legislation or government practices likely to affect the implementation of the action, including an offensive cyber/intelligence policy, pressure regarding place of manufacturing or access to information).
- (cyber-)security practices, including throughout the entire supply chain.
- risks identified in relevant assessments of Member States and third countries as well as other EU institutions, bodies and agencies, if relevant.

2. Equipment and other goods, works and/or services related to 5G/6G mobile network communication equipment, and other technologies linked to the evolution of European communication networks must:

- not be subject to security requirements by third country that could affect the implementation of the action (e.g. technology restrictions, national security classification limiting the use of the equipment, etc.).
- comply with (cyber-)security guidance issued by the Commission, in particular communications on the 5G toolbox.
- apply (cyber-)security requirements throughout the life cycle, including the selection and award procedure and criteria for purchases, the use, and also the related services, including installation, upgrading or maintenance.
- ensure (cyber-)security by adequately protecting the availability, authenticity, integrity, and confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, that equipment.

Exceptions may be requested from the granting authority and will be assessed case-by-case, taking into account the criteria provided for in the 5G cybersecurity toolbox, the security risks and availability of alternatives in the context of the action.

All actions under Article 12(6) of the Regulation (EU) 2021/694 and all actions under Specific Objective 3 - Cybersecurity and Trust also are subject to Appendix 4 restrictions, given the sensitive nature of the concerned activities, duly described and justified for each action in the respective section of the WP.

Appendix 5- Abbreviations and Acronyms

AI	Artificial Intelligence
AI/ML	Artificial Intelligence and Machine Learning
CBP	Cross-Border Platforms
CEF	The Connecting Europe Facility
CERT	The Computer Emergency Response Team
CRA	The Cyber Resilience Act
CSA	The Cybersecurity Act
CSAF	Common Security Advisory Framework
CSoA	The Cyber Solidarity Act
CSIRT	The Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
DORA	Digital Operational Resilience Act
EC	The European Commission
ECCC	European Cybersecurity Industrial, Technology and Research Competence Centre
ECSF	European Cybersecurity Skills Framework
EDIC	The European Digital Infrastructure Consortium
EDIH	European Digital Innovation Hub
EEA	The European Economic Area
EEA EFTA	The European Economic Area and the European Free Trade Association countries (Iceland, Liechtenstein, and Norway)
ENISA	European Union Agency for Cybersecurity

ERDF	The European Regional Development Fund
ERIC	The European Research Infrastructure Consortia
EUVDB	EU Vulnerability Database
GDPR	General Data Protection Regulation
IoT	Internet of Things
ISACs	Information Sharing and Analysis Centers
MCPs	Multi-Country Projects
MISP	Malware Information Sharing Platform
MS	Member States
NCCs	The Network of National Coordination Centres
NIS Directive	The Directive on Security of Network and Information Systems
NIS 2 Directive	Revised NIS Directive
OT	Operational Technology
PQC	Post-Quantum Cryptography
SIEM	Security Information and Event Management
SMEs	Small and Medium-sized Enterprises
SOC	Security Operation Centres
WP	Work Programme