DECISION No GB/2025/15

of The Governing Board of the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC)

on Amending the Digital Europe Cybersecurity Work Programme 2025-2027

THE GOVERNING BOARD,

Having regard to Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (hereinafter "the Regulation")[1], and in particular Article 13(3)(b), (c), and Article 25(7) thereof.

Having regard to Decision of the Governing Board of the ECCC No GB/2024/3, approving the Revision of Decision No GB/2023/1 on the ECCC's Financial Rules.

Having regard to Regulation (EU) 2021/6942[2] of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240.

Having regard to the Decision of the Governing Board of the ECCC No GB/2025/4, approving the ECCC Digital Europe Cybersecurity Work Programme 2025–2027 in March 2025.

Having regard to the Decision of the Governing Board of the ECCC No GB/2025/6, approving the Amendment 1 of the ECCC Digital Europe Cybersecurity Work Programme 2025–2027 in June 2025.

Whereas:

1. The Governing Board is empowered to amend the DEP Cybersecurity Work Programme 2025-2027 to ensure alignment with strategic objectives, operational developments, and budgetary adjustments.

2. During its latest meeting, the Governing Board discussed the need to revise the Work Programme to reflect the establishment of Regional Cable Hubs, the decrease of budget to facilitate contribution and investments into the AI Giga Factories, other improvements to the Work Programme text such as on the PQC Testing Facility, and an updated budget allocation table to reflect the changes..

[1] OJ L 202, 8.6.2021, p. 1-31.
[2] OJ L 166, 11.5.2021, p. 1–34.

3. The amendment aims to strengthen the coherence of the Work Programme, improve its operational relevance, and ensure efficient use of Union resources in accordance with the objectives of the Digital Europe Programme and the ECCC's mandate.

4. All these changes needed to be reflected with a GB decision.

HAS ADOPTED THE FOLLOWING DECISION:

Article 1

DECISION No GB/2025/4 is amended as set out in the Annex 1 of this decision.

Article 2

The present decision shall enter into force on the day of its adoption. It will be published on the ECCC's website.

Done at Bucharest, 9 October 2025

For the European Cybersecurity
Industrial, Technology and Research
Competence Centre

(e-signed)

Pascal Steichen
Chairperson of the Governing Board

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

ECCC Digital Europe Cybersecurity Work Programme 2025-2027

Consolidated Amendment 2, October 2025

Adopted by the GB of ECCC in Decision No 2025/15

VERSION HYSTORY

No.	Adoption	Changes
1	GB decision 2025/4	Adopted in March 2025
1.1	Amendment 1, GB decision 2025/6	Adopted in June 2025
2	Amendment 2, GB decision 2025/15	Adopted in October 2025

CONTACT

To contact the European Cybersecurity Competence Centre (ECCC) or for general enquiries, please use:

Email address: info@eccc.europa.eu

https://cybersecurity-centre.europa.eu/index_en

LEGAL NOTICE

This publication presents the consolidated amendment 2 of the ECCC Digital Europe Cybersecurity Work Programme 2025-2027, adopted in October 2025 by GB decision 2025/15, building on previously consolidated amendment 1 as approved by ECCC GB in June 2025, in Decision No GB/2025/6. The initial ECCC Digital Europe Cybersecurity Work Programme 2025-2027 was approved by ECCC GB decision 2025/04 in March 2025. The Governing Board may amend the DEP Work Programme 2025-2027 at any time. The ECCC reserve the right to alter, update or remove the publication or any of its contents.

This publication is intended for information purposes only. All references to it or its use as a whole or partially must refer to the ECCC as the source. Third-party sources are quoted as appropriate. The ECCC is not responsible or liable for the content of the external sources including external websites referenced in this publication. Neither the ECCC nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication. The ECCC maintains its intellectual property rights in relation to this publication.

Table of Contents

1 Introduction

In a changing geopolitical context, the EU is striving to strengthen its leadership and strategic autonomy in the area of cybersecurity. To achieve this, in December 2020, the Commission and the High Representative presented the EU's Cybersecurity Strategy for the Digital Decade[1], which sets out the objectives of developing the EU's technological sovereignty in cybersecurity, building capacity to secure sensitive infrastructures such as 5G, and reducing 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], in particular *Specific Objective 3: Cybersecurity and Trust,* is designed to co-invest in deploying research and development solutions from the cybersecurity domain, to multiply the effects on research results.

The European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) and the Network of National Coordination Centres (NCCs)[4] are pillars of the EU Cybersecurity Strategy. The ECCC is Europe's initiative to support innovation, industrial policy and research in cybersecurity. Together with the Member States and countries associated to Specific Objective 3 of the Digital Europe Programme (DEP), Cybersecurity Competence Community, the ECCC develops and implements 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 NCCs and the ECCC aim to enhance the EU's technological sovereignty by supporting projects in critical areas.

The Digital Europe Programme supports the co-investment strategy provided in Regulation 2021/887 establishing the ECCC. Until 2023, the DEP Work Programmes (WP) on Cybersecurity for 2021-2022[6], for 2023-2024 and the amendment of the latter[7], were developed under the leadership of the European Commission.

---

[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] Regulation (EU) 2021/694 of the European Parliament and of the council of 29 April 2021 establishing the Digital Europe Programme repealing Decision (EU) 2015/2240 (hereinafter the 'DEP Regulation').
[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 Competence Centre and the Network of National Coordination Centres.
[5] ECCC Strategic Agenda available at: https://cybersecurity-centre.europa.eu/strategic-agenda_en.
[6] Available from the page: The DIGITAL Europe Programme – Work Programmes | Shaping Europe's digital future
[7] Amended DEP Cybersecurity WP for 2023-2024, available at: https://ec.europa.eu/newsroom/dae/redirection/document/100739.

The DEP will facilitate the deployment of cybersecurity solutions and will ensure uptake of the research results delivered by the Horizon Europe programme (HEP), which is dedicated to financing European research.

Article 12(5) of the DEP Regulation restricts participation to entities established in and controlled from eligible countries (Appendix 3)[8]. The Cyber Solidarity Act[9], provides for amendments to Article 12(5) and (6) of the DEP Regulation by allowing for flexibility beyond the provisions of Article 12(5) (i.e. purchasing from non-EU controlled companies). This will be based on a biennial (at least every two years) mapping by ECCC of tools, infrastructures and services needed by Cyber Hubs, including their availability from EU established and EU controlled entities[10]. The first mapping exercise pursuant to Article 9(4) of the Cyber Solidarity Act, to be conducted in consultation with the CSIRTs Network, the existing Cross-border Cyber Hubs, ENISA and the Commission, is ongoing. Until the mapping is completed and in line with the relevant provisions of the Cyber Solidarity Act, participation to the calls funded under this topic will be therefore subject to the restrictions of Article 12(5), as specified in Appendix 3 of this Work Programme. These security conditions may be later amended taking into account the results of the final mapping of services carried out by the ECCC pursuant to Article 9(4) of the Cyber Solidarity Act.

The aim of the Work Programme (WP) 2025-2027 is to cover the remaining actions and budget dedicated to *Specific Objective 3: Cybersecurity and Trust* foreseen in the DEP Regulation and to be implemented by the ECCC. This Cybersecurity WP is meant to complement the main DEP WP.

This is the first DEP WP developed by the 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

[8] 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).

[9] Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act)

[10] The decision to apply Article 12(5) or (6) of the DEP Regulation will be done following the assessment of the results of the mapping exercise provided in the Cyber Solidarity Act and initiated by the ECCC in Q4/2024.

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

Directive, etc. The document is also aligned with the priorities of the new EU Commission relating to cybersecurity, as presented in the Political Guidelines 2024-2029[12].

It should be noted that, in order to achieve the ambitious objectives set out in the ECCC Regulation and efficiently reinforce the EU's strategic autonomy in cybersecurity, it is important to connect research, innovation, maturation and deployment in a coherent way. For this reason, a more direct involvement of the ECCC in the preparation and call management of the HEP work programme will improve synergies and ensure optimal use of resources.

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 (NIS 2).** 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 are to be applied from 18 October 2024. The new Directive raises the EU's common level of ambition on cybersecurity, 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)[13]. The CRA establishes a horizontal legal framework for cybersecurity essential 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. The Cyber Resilience Act, Regulation (EU) 2024/2847[14] entered into force in 2024.
- **Cyber Solidarity Act.** In April 2023, the Commission adopted a proposal for a Cyber Solidarity Act, including amendments to the DEP 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. The Cyber Solidarity Act[15] entered into force on 4 February 2025. The Cyber Solidarity Act provides for a number of actions for the ECCC to implement. The ECCC will be

[12] President-elect Von Der Leyen presented her Political Guidelines 2024-2029 before the European Parliament Plenary on 18 July 2024: https://commission.europa.eu/about-european-commission/president-elect-ursula-von-der-leyen_en.
[13] Proposal for a 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.
[14] Regulation (EU) 2024/2847, Cyber Resilience Act, available at: http://data.europa.eu/eli/reg/2024/2847/oj
[15] Regulation (EU) 2025/38, Cyber Solidarity Act, available at: https://eur-lex.europa.eu/eli/reg/2025/38/oj

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 is 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 for 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 Framework**. 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. The amendment of the Cybersecurity Act, enabling the future adoption of European cybersecurity certification schemes for managed security services, entered into force on 4 February 2025. The first European Cybersecurity Certification Scheme, the Common Criteria-based European cybersecurity certification scheme (EUCC) has been adopted, and two 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, from developing harmonised evaluation methodologies and promoting innovation to testing ICT products, services and processes.
- **EU 5G Toolbox.** The EU 5G Toolbox[17] is a non-binding comprehensive and objective risk-based approach for the security of 5G and future generation networks. In June 2023, the NIS Cooperation Group adopted a report on the implementation status 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

[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).
[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.

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 programmes. The respective work programmes for 2023 and 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 upscaling of European cybersecurity industry.
- **European action plan on the cybersecurity of hospitals and healthcare providers**. As part of the Political Guidelines of the 2024-2029 Commission mandate, the action plan focuses on improving threat detection, preparedness, and response in the healthcare sector[22]. It aims to provide tailored guidance, tools, services, and training to hospitals and healthcare providers. Several specific actions[23] will be rolled out, in collaboration with health providers, Member States, and the cybersecurity community.
- **European Action Plan on Cable Security** aims to strengthen the security and resilience of submarine cables[24]. The Joint communication published in February2025 presents strong actions in a whole resilience cycle approach: prevent, detect, respond and repair, and deter.

---

[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.

[22] 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.

[23] EC Communication available here: https://ec.europa.eu/newsroom/dae/redirection/document/111664; published on 15 January 2025.

[24] *Joint Communication to strengthen the security and resilience of submarine cables*, published on 21 February 2025, available at: https://digital-strategy.ec.europa.eu/en/library/joint-communication-strengthen-security-and-resilience-submarine-cables and *EU Action Plan on Cable Security: mapping and risk assessment approach agreed by Group of Member States and Commission experts*, published on 24 June 2025, available at: https://digital-strategy.ec.europa.eu/en/node/13895/printable/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 DEP will strengthen the preparedness and resilience of the key sectors and response actions across the EU to defend against cyber threats. Cybersecurity solutions can improve the resilience and security of critical infrastructures for global communications, including submarine cables in line with the Joint Communication of the European Commission and the High Representative for Foreign Affairs and Security Policy to strengthen the security and resilience of submarine cables[25].The DEP 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 secure their implementation. This will facilitate the deployment of **Artificial Intelligence and cybersecurity**: financing the uptake of AI, including generative AI, cybersecurity of AI and AI for cybersecurity, tools and other key digital technologies for cybersecurity applications, as well as for improving and expanding the capabilities of Cyber Hubs, while also contributing to strengthening European cyber resilience. It will also contribute to the **post-quantum transition** by supporting the adoption Post Quantum Encryption technologies for industry and public administrations.
- Deliver the **Cyber Solidarity Act** and **EU Action Plan on Cable Security**. These actions will contribute to the consolidation of the **European Cybersecurity Alert System**: supporting the deployment of Cyber Hubs and Cross-Border Cyber Hubs in line with the recently adopted Cyber Solidarity Act will support detection and enhance awareness regarding cybersecurity threats. They will implement the **Cybersecurity Emergency Mechanism** and support **preparedness actions** across 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 supporting also **mutual assistance** between Member States, in the context of the Cyber Solidarity Act. In addition, the establishment of dedicated regional cable hubs will

[25] Commission and High Representative present strong actions to enhance security of submarine cables.

strengthen the **cybersecurity of submarine cables** in line with the EU action plan presented by the Commission.

- Support **additional policy implementation activities to improve EU resilience**, including the implementation of NIS 2 and the Cyber Security Act as well as the Cyber Resilience Act, while providing SMEs with the tools to comply with regulatory requirements. Support will be provided to industry, SMEs and start-ups to comply with regulatory requirements, especially the NIS 2[26] implementation or requirements concerning the Cyber Resilience Act[27]. 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 at the European Parliament Plenary on 18 July 2024[28] and recent Action Plan on the Cybersecurity of Hospitals and Healthcare providers[29]. Support will also be provided for solutions to cover the surveillance and **protection of critical undersea infrastructure**, such as submarine cables, and the detection of malicious activities around them, to improve the resilience and security of this infrastructure, which is critical for global communications.

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[30] is not alone in pursuing these objectives, as it is complemented by actions in the main Digital Europe WP implemented by the European Commission and other EU bodies and agencies.

---

[26] See Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, available at: https://eur-lex.europa.eu/eli/dir/2022/2555.

[27] See Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU), 2019/1020, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0454.

[28] 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.

[29] From January 2025, available at: https://ec.europa.eu/newsroom/dae/redirection/document/111664.

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

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 approximatively EUR **355 million**[31], distributed across 3 years from 2025 to 2027.

This value has been reduced from the initial approved budget of EUR **390 million** due to reallocation of EUR **35 million** for the support of the AI Gigafactories as discussed by the ECCC Governing Board during its meeting on 2-3 July 2025**.**

The updated **indicative** proposal for the distribution of the budget for the period is as follows.

- EUR 139 million for **new technologies and cybersecurity**, the deployment of Artificial Intelligence & cybersecurity and the post-quantum transition**.**
- EUR 97 million for the **implementation of Cyber Solidarity Act**, consolidation of **European Cybersecurity Alert System, Cybersecurity Emergency Mechanism/preparedness actions**, **mutual assistance** and establishment of **regional cables hubs.**
- EUR 110 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 decisions; Section 1.6 provides a tentative allocation for the period 2025-2027.

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.

[31] This amount covers the initially allocated DEP budget for 2025-2027 of EUR 353 million (reduced to EUR 348 million) and an additional amount of EUR 42 million carried over from 2022 in line with the ECCC financial rules. The exact values are presented in the adopted SPD 2025-2027, GB decision 2024/13, available at: https://cybersecurity-centre.europa.eu/system/files/2025-01/ECCC%20GB%20Decision%20No%202024_13%20Final%20SPD%202025-2027.pdf.

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 in some of the calls funded under this WP may be, depending on the topic, subject to the provisions of Article 12(5) of the DEP Regulation, as indicated in each corresponding 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 the conclusion/performance of the Mapping in accordance with the Cyber Solidarity Act, the text of the calls will be amended to reflect the results of the assessment initiated in Q4/2024 and set the security conditions accordingly for National and Cross-Border Cyber Hubs.

1.5.2 Links to programmes and co-investments

Most of the actions provided under the DEP require co-investments from the public and private sectors. The terms of these co-investments are described in the corresponding parts of the various work programmes.

As far as 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. The relevant provisions of the Financial Regulation need to be respected[32]: the same costs may under no circumstances 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

[32] In particular Article 191: Principle of non-cumulative award and prohibition of double funding.

must be compatible with EU State aid rules as described in Appending 6 on State Aid of the Main DEP Work Programme pages 199-203, C(2025) 1839[33].

Alternating/sequenced funding is possible when each instrument finances a different part, or successive parts, of the operation/action. For this, an operation/action must be split in two different parts. Separate grant agreements are required, following the rules of each of the funding instruments. Coordination is required to avoid double funding, ensuring the separation of parts/activities. Expenditure used for a reimbursement request for one instrument cannot 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 need to be followed, starting with preparation, the linking of actions, grant signatures all the way to reporting and payments. The Commission Notice on Synergies between the Horizon Europe Programme and the European Regional Development Fund (ERDF) programmes[34] 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 the 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.

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.

[33] Main DEP WP, C(2025) 1839, available: https://ec.europa.eu/newsroom/dae/redirection/document/114219
[34] Synergies between Horizon Europe and the ERDF programmes (2022), available at: https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/synergies-guidance-out-2022-07-06_en.

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 % for procurement 50 % for grants 70 % for grants related to regional cable hubs
AI, PQC, preparedness, others	50 %

1.5.3 Multi-Country projects and the European digital infrastructure consortia

As part of the 'Path to the Digital Decade' policy programme proposal[35], 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[36]. They channel coordinated investments between the EU, Member States and private stakeholders, for example to 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 an 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 MCP areas are within the scope of the Digital Europe Programme and are receiving funding under the Digital Europe Main WP 2021-2022, 2023-2024 and Cybersecurity WP.[37] The MCPs in this WP are dedicated to Cyber Hubs, as described in section 2.7.

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, as set out in Article 107(1) TFEU, are met.

1.5.4 Climate and biodiversity

Digital tools have the potential to contribute to the energy transition and climate change. Through interconnected technologies, AI can be an enabler for low-carbon smart cities and

[35] Proposal for a Decision establishing the 2030 Policy Programme 'Path to the Digital Decade', available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0574.
[36] Digital Compass: the European way for the Digital Decade, available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118.
[37] The initial list of areas of activity for Multi-Country projects, as per the 'Path to the Digital Decade' Policy Programme Annex is listed in Annex 4 (Section 9.4) of the Main WP 2023-2024.

ensure that energy consumption is efficient; digital services remove the need for physical presence; data spaces can provide data to organisations to help them improve efficiency; security by design and smart grids could reduce energy consumption in specific sectors. Cybersecurity infrastructures, connected devices 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 cyberattacks. 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 contribute directly to the conservation and restoration of biodiversity (ecosystems, species, and genetic diversity), but to the maintenance of related ecosystem services, to the sustainable use and management of biodiversity and ecosystems (including activities within agriculture, forestry, fisheries and other sectors), and to the fair and equitable sharing of the benefits arising from genetic resources.

1.6 Calls structure and planning

This section lists all the proposed topics for 2025-2027. The topics are clustered into broad interconnected areas, and many of them are dedicated to the implementation of EU legislation on cybersecurity. While some topics are dedicated to specific public entities – such as those acting as Cyber Hubs – many others are designed to support SMEs.

Provided below is the list of areas:

- **New technologies and cybersecurity**: impact and benefits of AI and post-quantum transition on cybersecurity.
- **Cyber Solidarity Act**, European Cybersecurity Alert System, Cybersecurity Emergency Mechanism and Mutual Assistance and implementation of the EU Action Plan on Cable security.
- Implementation of EU legislation dedicated to **EU resilience**, including topics targeting sectorial priorities and strengthening capabilities of NCCs.

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

Areas and topics with indicative allocations (in million EUR)		2025	2026	2027	Total
New technologies, AI & post-quantum transition					**139**
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			4	4
2.6	Uptake of innovative cybersecurity solutions for SMEs	15		15	30
Cyber Solidarity Act and EU Action Plan on Cable Security Implementation					**97**
2.7	National Cyber Hubs	5	5		10
2.8	Cross-Border Cyber Hubs	5		15	20
2.9	Strengthening the Cyber Hubs ecosystem and enhancing information sharing		2		2
2.10	Coordinated preparedness testing and other preparedness actions	10	15	15	40
2.11	Mutual assistance		2	2	4
2.12	Regional Cable Hubs	10	5	6	21
Additional actions improving EU cyber resilience					**110**
2.13	Enhancing the NCC Network	10	11	17	38
2.14	Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements		20	12	32
2.15	Dedicated action to reinforce hospitals and healthcare providers	30			30
2.16	Dual-use technologies		10		10
Programme Support Actions		3	3	3	9
TOTAL (in million EUR)		**143**	**108**	**104**	**355**

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

Main tasks	Tentative timeline
Opening	Q2/2025 and Q4/2025
Closing	Q4/2025 and Q1-Q2/2026
Evaluation	Q1/2026 and Q3/2026
Signature of the grants	Q3/2026 and Q1/2027

2 Deployment actions in the area of cybersecurity

New technologies, AI & post-quantum transition

Several topics are presented under this area. Some concern the requirements of public bodies and their needs in terms of cybersecurity, where AI could enable more efficient and effective solutions and ensure a smooth transition to post-quantum cryptography (PQC). 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 post-quantum transition. Cybersecurity is the precondition for reliable, secure and resilient AI models and algorithms to be used and deployed under these 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-based technologies (including GenAI) for national authorities and competent authorities, including National and Cross-Border Cyber Hubs, CSIRTs, public bodies and private entities from the NIS 2 directive, NCCs[38], etc. They play a key role in providing central operational capacity to European cybersecurity ecosystems. They may also provide primary input data for AI/ML-based cybersecurity tools and solutions, which can strengthen such authorities' capacity 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 generative AI[39] could be a challenge and an opportunity for cybersecurity[40] processes and applications.

These enabling technologies should allow for 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, especially for the systems in the learning phase, also needs to be addressed, including the misuse of AI by malicious actors. This includes carrying out risk

[38] If applicable and in line with individual national strategies.
[39] 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.
[40] 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.

assessments and mitigation of cybersecurity risks inherent to AI technologies, implementing supply chain security, etc., and complying with the AI Act, intellectual property legislation and the GDPR.

In addition to being secure, the AI technologies being developed should perform well, and be robust and trustworthy. In particular, having trustworthy AI solutions will help in the deployment phase, where social acceptance is essential.

2.1.2 Scope

Actions in this topic should develop and deploy systems and tools for cybersecurity[41], based on AI technologies[42], 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 of vulnerabilities and support for management considering multiple sources of information.
- Cybersecure tools and solutions that provide risk-reduction in the crossover between AI, IoT and smart grids or other manufacturing chains.
- 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.

[41] 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.
[42] Cybersecurity of AI and Standardisation, ENISA, March 2023, available at: https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation.

- Enabling organisations to leverage and share CTI and other actionable information for analysis and insights without compromising data security and privacy, through anonymisation.
- Tools and solutions that provide product security or cybersecurity by design/default in line with CRA requirements.
- Tool and service providers are welcome to apply for 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 cases, access requests to the EuroHPC high performance computing infrastructure could be granted.
- The systems, tools and services developed under this topic will be made available for licensing 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 their crucial operative role in ensuring cybersecurity in the Union, the nature of the technologies involved as well as the sensitivity of the information handled, Cyber Hubs 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 and considering integration of requirements for robustness, performance, trust and balanced AI autonomy.
- 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 standardised, transparent, and rigorous certification process, the EU seeks to foster trust in AI technologies among users, developers, and regulators alike.

2.1.3 Expected Outcome

- 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 that have been 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 the creation, analysis and processing of CTI, to enhance operations of the Cyber Hubs.
- Original European CTI feeds or services.
- Ensure that 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	*EUR 45 million*
Indicative call planning	2025, 2026, 2027
Indicative duration of the action	3 years
Implementation	ECCC
Types of Beneficiaries	Technology providers, operators of Cyber Hubs, Research and academia, cybersecurity entities, Public sector, NIS 2 Directive entities, private sector, Other relevant stakeholders supporting the deployment of cyber-secure AI solutions.
Security	Call restricted on the basis of Article 12(5) of the DEP Regulation (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 an understanding of the evolving technology landscape, of the benefits of technology integration and of deployment prioritisation. 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 cyberattacks, as required by the EU's AI Act for high-risk AI systems. The need for human oversight of AI has also been emphasised 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 SMEs in the EU. Actions in this topic should develop and deploy AI-powered products, tools and services for European SMEs, also enabling the detection/discovery of attack patterns.

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 SMEs to improve the key aspects of their cybersecurity by providing user-friendly tools for risk management[43], 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-incident prediction and response functions to improve SMEs' 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 sets 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.

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

- 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.

2.2.3 Expected Outcome

- 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, including providing innovative approaches to training employees to use AI solutions for cybersecurity.
- Deployment of cybersecure tools and technologies relying on trustworthy AI; AI-driven cybersecurity tools; Integration of tools to protect and secure AI solutions.

Type of action	SME support action
Indicative budget	*EUR 20 million*
Indicative call planning	2026
Indicative duration of the action	3 years
Implementation	ECCC
Types of Beneficiaries	SMEs, start-ups, research and academia Public sector, NIS 2 Directive entities Other industry actors and related stakeholders (including providers of AI-assisted functionalities)
Security	Call restricted based on Article 12(5) of the DEP Regulation (2021/694).

Deployment of post-quantum cryptography

The advances in quantum technologies[44], 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 have the potential to break current

[44] 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/.

asymmetric cryptographic protocols and weaken current symmetric ones. With their advent, the known algorithms Rivest-Shamir-Adelman (RSA) and Elliptic Curve Cryptography (ECC)[45], 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.

The threats already exist now. Data may be captured and stored today, waiting to be decrypted later when quantum computers will become available. Therefore, the time that sensitive data needs to remain confidential needs to be considered as well. Moreover, many of the electronic devices and systems in production today do not have quantum-resistant capabilities and could have lifetimes that span 10 years or more, extending into the timeframe when quantum computers are anticipated to be in commercial use.

The whole digital infrastructure is impacted by such threats. 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 from 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 a countermeasure to quantum threats.

The transition to PQC[46,47] 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 standardised[48] and will continue to be standardised in the near future. However, they may arrive with unknown interoperability and performance issues or side-channel vulnerabilities. It is of utmost importance to begin testing for PQC deployment in Europe for the proper functioning of our society, to prepare it for the full transition to PQC, as this could help to identify and address unforeseeable technical and logistical challenges.

Ensuring connectivity and interoperability between organisations, 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-

[45] https://www.techtarget.com/searchsecurity/definition/elliptical-curve-cryptography.
[46] 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.
[47] 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.
[48] 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.

quantum public-key algorithms. Also, the creation of collaboration platforms for testing, shared between SMEs, start-ups, public organisations, academia, PQC product suppliers and service providers, and larger corporations, will accelerate the transition of all European actors and will help bring trustworthy PQC solutions to market, while benefiting from the innovations 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 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 incorporate best practices and lessons learnt to initiate their own transition and lead by example in the EU's efforts to deploy 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 European global benchmark testing infrastructure for the transition to PQC, accessible to different kinds 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 to better support the design of tests and evaluation of results, as well as to public organisations and to members of large European industry organisations to facilitate 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

The aim is to create, operate and maintain a European PQC testing infrastructure. The testing infrastructure should offer a physical space for in-situ testing, possibly centralised or distributed in 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. Results from ongoing activities in the EU should be considered, when possible.

The PQC testing infrastructure should ensure the necessary facilities and the availability of state-of-the-art tools to allow European users to test PQC deployments in a trusted environment and should facilitate and support access by European industry, with a specific

focus on SMEs. The infrastructure governance should ensure fairness in access to the facilities by different users, and data management practices.

A major challenge to be addressed is maintaining connectivity and interoperability among organisations 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, facilitating the successful market adoption of such solutions.

The development of digital twin solutions mimicking specific critical infrastructure behaviour could also be envisaged, aiming at training for the transition and realising impact analyses.

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 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, development of a catalogue of tests, and of 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.

The acquisition of infrastructure, tools, and services will take place through a competitive procurement process open to European industry players, with possible participation of public organisations, and academia and research institutions.

Ownership of the tools, services and infrastructure purchases as part of the procurement and outcomes or results generated will remain with the ECCC. Operational support will be ensured by the selected providers following the procurement process.

Participation of non-EU entities to the procurement procedure 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.
- Maintenance and operation of the testing infrastructure.
- 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 eventual testing of innovative solutions, combining technologies of different types, such as new quantum random number generators (QRNGs) and PQC.

Type of action	Procurement
Indicative budget	*EUR 25 million*
Indicative call planning	2025
Indicative duration of the action	4 years
Implementation	ECCC
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 offers efficient migration strategies and strong business continuity guarantees.

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 business continuity, in a broad range of applications relevant for critical societal sectors and processes (such as governmental services, telecom, banking, smart homes, e-Health, automotive, and other sectors).

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. The proposed systems should be able to seamlessly interact with legacy systems by disabling the post-quantum component as needed while preventing downgrade attacks. Relying solely on PQC solutions in this intermediate transition phase could introduce security risks given that the security analysis of the cryptosystems and of their implementations is not as mature as for their pre-quantum counterparts. Proposals should therefore use combinations of PQC solutions and established pre-quantum solutions, making sure to provide strongest-link security, meaning that the system remains secure as long as at least one of the components of the combination is secure.

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 decentralised 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, standardisation, policy, and application deployment, as well as organisations 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 optimisation 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. Support to standardisation activities.
- 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 specialised 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, emphasising 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 training courses.

Type of action	Simple grant
Indicative budget	*EUR 15 million, (grant of EUR 4 to 5 million)*
Indicative call planning	2025
Indicative duration of the action	3 years
Implementation	ECCC
Types of Beneficiaries	All actors in PKI chain
Security	Call restricted based on Article 12(5) of the DEP Regulation (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 European Cybersecurity Certification Group (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.

- Liaising with ENISA for the work done in the context of the ECCG on certification, the NIS Cooperation Group, 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 programmes.

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 in line with the PQC Work Stream in the NIS Cooperation Group.
- 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	*EUR 4 million (grant of EUR 1 million to EUR 2 million)*
Indicative call planning	2027
Indicative duration of the action	3 years
Implementation	ECCC
Types 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 DEP Regulation (2021/694).

2.6 Uptake of innovative cybersecurity solutions for SMEs

The action aims at improving industrial and market readiness for the cybersecurity requirements for SMEs as specified in relevant EU cybersecurity legislation, for instance, as set in the Cyber Resilience Act ensuring more secure hardware and software products.

2.6.1 Objectives

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

- Availability of innovative tools and services that support SMEs in complying with the EU cybersecurity legislation.
- Availability of innovative tools and services that support SMEs in reporting incidents and in assisting with recovery if possible, and in exchanging with competent authorities (i.e. cooperation with Cyber Hubs, CSIRTs (including in relation to the CSIRT Network) and/or ISACs, for e.g. 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.
- Industrial and market readiness for the proposed Cyber Resilience Act.
- Support for Cybersecurity certification in line with the Cybersecurity Act.
- Support for supply chain partners in standardised self-assessments and certifications. Helping downstream supply chain partners in a step-by-step approach to increase 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[49] 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.

2.6.2 Scope

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

2.6.3 Expected Outcomes

The development of a cyber toolkit as a service to support SMEs managing cyber risks, defining, and implementing their cybersecurity strategy. The toolkit could include at least one of the following:

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

- Interfaces that will connect to existing SaaS applications such as HR, invoice and financial management, CRM and accounting systems, etc., which are often used by SMEs for increasing their cybersecurity.
- A functionality that enables the mapping and maintenance of an SME's digital assets and possible vulnerabilities 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 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.
- Tools supporting detection, prevention and response in Operational Technology infrastructures using open standards or technologies.

Support and incident response capabilities to SMEs:

- Non-commercial cybersecurity hotline with a standardised 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.
- Specialised 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	EUR 30 million (EUR 15 million in 2025 and EUR 15 million in 2027)
Indicative call planning	2025, 2027
Indicative duration of the action	3 years
Implementation	ECCC
Types 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 DEP Regulation (2021/694).

Cyber Solidarity Act and EU Action Plan on Cable Security implementation

European Cybersecurity Alert System

In a context of accelerated digitisation and in view of 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, so as 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 of supporting 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 specified in the Cyber Solidarity Act, 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 provides, 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. Support is also planned

for the development and consolidation of the National Cyber Hubs and the Cross-Border Cyber Hubs, which 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 interlinking via Cross-Border SOCs. While the *Cyber Solidarity Act*[50] 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 continued objective of supporting joint actions to create an advanced (state-of-the-art) threat detection and cyber early warning ecosystem. This objective aims 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 the signals detected more efficiently and more rapidly, 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. The different steps related to the implementation of these actions (e.g. CfEI, Joint Procurements and Grant Agreements) will be detailed in the call for proposal.

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[51], the Cybersecurity Act[52], the Cyber Resilience Act[53] and the Cyber Solidarity Act. The proposed actions will support the implementation of the Cyber Solidarity Act, and the establishment of a Cybersecurity Emergency Mechanism

[50] http://data.europa.eu/eli/reg/2025/38/oj.
[51] See https://eur-lex.europa.eu/eli/dir/2022/2555.
[52] See https://eur-lex.europa.eu/eli/reg/2019/881/oj.
[53] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0454.

designed to support Member States, upon request, in preparing for, responding to, and initially recovering from significant and large-scale cybersecurity incidents.

Technical Mutual Assistance

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

EU Action Plan on Cable Security

Following a series of incidents in the Baltic Sea, the European Commission presented an Action Plan on Cable Security in June 2025 for all the sea basins and based on a full-cycle resilience approach: prevent, detect, respond/repair & deter. As part of the detect pillar, the Commission proposes the establishment of integrated surveillance mechanisms to enhance the security of undersea cables through Regional Cable Hubs. These Regional Cable Hubs are designed to act as a platform to gather all the necessary information – a sea basin level – for the specific security of undersea cables. There are many surveillance systems, information and data which today are not connected and not used towards the specific security of undersea cables. The Regional Cable Hubs should build on existing systems and develop a dedicated surveillance layer for undersea cables to establish a near real time situational picture. Additionally, these hubs should act as a platform for reporting incidents and sharing the information in a secured way at regional level to enhance the operational security & the response time. Finally, the Action plan foresees also increased cooperation with the private sector to enhance detection capacities as well as a progressive integration of the defence dimension.

In that sense, these connected surveillance systems, information and data, as well reporting incidents and information sharing platforms should take into consideration cybersecurity practices and technologies.

The EU Action Plan on Cable Security is an urgent priority for the European Union for the importance that these critical infrastructures have for global communications and power supply and in consideration of the pressing security threat that underseas cables are facing.

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 of preventing 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. National Cyber Hubs could also consider the possibility of monitoring undersea infrastructure, such as submarine cables.

2.7.2 Scope

The aim is to build capacity 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, such as the Common Security Advisory Framework (CSAF)[54], for security advisories or for collecting and processing cybersecurity-related messages (e.g. IntelMQ project[55]). Applications developed by Cyber Hubs/SOCs should be compatible with European standardisation projects like the EU vulnerability database (EUVD). National 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

[54] 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.
[55] IntelMQ: https://github.com/certtools/intelmq.

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.

Furthermore, National Cyber Hubs could also consider deploying solutions for the surveillance and protection of critical undersea infrastructure, such as submarine cables, and the detection of malicious activities around them, to improve the resilience and security of this infrastructure, which is critical for global communications. The response to such hybrid threats could also include situational awareness performed through the collection and analysis of in-situ, sea based sensor data as well as relevant satellite imagery. For such activities, operational synergies with the EU Copernicus Space Programme and in particular with its Security Service are required.

Another key role for National Cyber Hubs is to facilitate knowledge transfer and sharing, as well as support training initiatives for all needed cybersecurity roles the basis, for instance, of the European Cybersecurity Skills Framework (ECSF[56]). 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[57] 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 Hub, describe its role and how such role relates to other cybersecurity actors, such as CSIRTs, and its potential cooperation with other public or private cybersecurity stakeholders. Applicants should also provide the detailed planning of the activities and tasks of the National Cyber Hub, the services it will offer, the way it 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 Hub, its services and its infrastructure.

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

- **[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.

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

[57] 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.

- **[Building up and running the National Cyber Hub]** A grant will also be available to cover, among others, the preparatory activities for setting up the National Cyber Hub, its interaction and cooperation with other stakeholders, as well as the running/operating costs involved, enabling the effective operation of the National 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. The applications will be subject to an evaluation procedure. 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, in cooperation with other relevant national/regional entities, are tasked with monitoring, understanding and proactively managing cybersecurity threats. Cyber Hubs will have a crucial operative role in ensuring cybersecurity in the Union and will handle sensitive information.

Pursuant to Article 12(5a) of the Cyber Solidarity Act amending Article 12 of Regulation (EU) 2021/694, Article 12(5) of Regulation (EU) 2021/694 shall not apply if the conditions stipulated in Article 12(5a) are cumulatively met. The assessment of these conditions should take into account the results of the mapping of the availability of tools, infrastructure and services for the National Cyber Hubs to be carried out by the ECCC pursuant to Article 9(4) of the Cyber Solidarity Act.

The first mapping exercise is ongoing. Until the mapping is completed and in line with the relevant provisions of the Cyber Solidarity Act, participation to the calls funded under this topic will be therefore subject to the restrictions of Article 12(5), as specified in Appendix 3 of this Work Programme. These security conditions may be later amended taking into account the results of the final mapping of services carried out by the ECCC pursuant to Article 9(4) of the Cyber Solidarity Act.

2.7.3 Expected Outcomes

World-class National Cyber Hubs across the Union, supported by state-of-the-art technology, acting as clearing houses 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 training courses on the basis of the ECSF to improve the capacity of cyber security roles.
- 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	*EUR 10 million* - 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
Types of Beneficiaries	Public bodies acting as National Cyber Hubs, as identified by Member States
Security	Action restricted on the basis of Article 12(5) of the DEP Regulation (2021/694). 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 Proposals- 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
Types of Beneficiaries	Successful applicants to the workstream on joint procurement
Security	Action restricted on the basis of Article 12(5) of the DEP Regulation (2021/694). 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	*EUR 3 343 961.00* - 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
Types 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: EUR 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-Border 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 is aimed mainly at new Cross-Border Cyber Hubs. Supporting activities for the SOCs that were already launched under the previous DIGITAL work programmes (2021-2022 and 2023-2024)[58] could also be included when relevant to ensure collaboration with the Cross-Border Cyber Hubs.

In addition to setting up processes, tools and services for prevention, detection and analysis of emerging cyberattacks, 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[59]) or automation of advisory information (e.g. CSAF[60]) and cybersecurity related messages (e.g. by IntelMQ) should be considered. Cross-Border Cyber Hubs could also foresee the possibility to monitor undersea infrastructure, such as submarine cables.

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.

[58] ENSOC and ATHENA consortia are already financed.
[59] MISP Standard: https://www.misp-standard.org/.
[60] 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.

The platforms should act as a central point allowing for broader pooling of relevant data and CTI, enabling the dissemination 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 procedural arrangements on cooperation and sharing of relevant information and on the types of information to be shared.

Furthermore, Cross-Border Cyber Hubs could also deploy solutions for the surveillance and protection of critical undersea infrastructure, such as submarine cables, and the detection of malicious activities around them, to improve the resilience and security of this infrastructure, which is critical for global communications. The response to such hybrid threats could also include situational awareness performed through the collection and analysis of in-situ, sea based sensor data as well as relevant satellite imagery. For this activity, operational synergies with the EU Copernicus Space Programme and in particular with its Security Service are required.

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 the authorities in the Member States and to the Commission through the EU-CyCLONe and the CSIRTs network[61], 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 potential 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 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.

[61] As defined by Directive (EU) 2022/2555.

- **[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, personnel. These will also indicate milestones and deliverables to monitor progress.

Applications shall be made to both workstreams. The applications will be subject to an evaluation procedure. 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 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 in ensuring cybersecurity in the Union and will handle sensitive information.

Pursuant to Article 12(5a) of the Cyber Solidarity Act amending Article 12 of Regulation (EU) 2021/694, Article 12(5) of the Regulation (EU) 2021/694 shall not apply if the conditions stipulated in Article 12(5a) are cumulatively met. The assessment of these conditions should take into account the results of the mapping of the availability of tools, infrastructure and services for the Cross-Border Cyber Hubs to be carried out by the ECCC pursuant to Article 9(4) of the Cyber Solidarity Act.

The first mapping exercise is ongoing. Until the mapping is completed and in line with the relevant provisions of the Cyber Solidarity Act, participation to the calls funded under this topic will be therefore subject to the restrictions of Article 12(5), as specified in Appendix 3 of this Work Programme. These security conditions may be later amended taking into account the results of the final mapping of services carried out by the ECCC pursuant to Article 9(4) of the Cyber Solidarity Act.

2.8.3 Expected Outcomes

- 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	*EUR 20 million* -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
Types of Beneficiaries	Public bodies acting as National Cyber Hubs, as identified by Member States.
Security	Action restricted on the basis of Article 12(5) of Regulation (EU) 2021/694. 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 Proposals – 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
Types of Beneficiaries	Successful applicants to the workstream on joint procurement
Security	Action restricted on the basis of Article 12(5) of the DEP Regulation (2021/694). 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 Cyber Hubs 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 in relation to National Cyber Hubs and other Cyber Hubs, and in the absence of Cyber Hubs in the relevant Member State authorities.
- Fostering links between public sector and industry, and stimulating mutually beneficial exchange of information, tools and data as well as exchange of knowledge and training opportunities.
- 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 those developed in Sections 2.1-2.6 of this work programme dedicated to AI and post-quantum technologies) and knowledge exchange.
- Supporting notifications 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 in 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 Expected Outcomes

- 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. Promoting cooperation and integration with the network of ISACs and other EU initiatives (e.g. CSIRT network and Cyber Hubs) toward a common and integrated situational awareness.
- Develop standardised approach for exchanging information and reporting/compliance[62]. Technical frameworks and mappings of taxonomies to allow for information exchange between Cross-Border Cyber Hubs.
- Develop and share training courses, including competitions such as Capture the Flag (CtF), on the basis of the ECSF, and exercises to strengthen cooperation among Cyber

[62] Information sharing formats and protocols should be guided by and therefore take as their starting point the guidelines issued by ENISA, pursuant to the Cyber Solidarity Act.

Hubs SOCs, ISACs and other EU initiatives and facilitate the sharing of information and notifications.

- Framework to facilitate the exchange[63] 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	*EUR 2 million*
Indicative call planning	2026
Indicative duration of the action	2-3 years
Implementation	ECCC
Types of Beneficiaries	Cyber Hub operators
Security	Call for grants and procurement are restricted on the basis of Article 12(5) of the DEP Regulation (2021/694).

2.10 Coordinated preparedness testing and other preparedness actions

This action covers two actions from the Cyber Solidarity Act, dedicated to the 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 their preparedness for cyber threats and incidents by providing them with knowledge and expertise.

Proposals should contribute to achieving at least one of the following 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 training courses).

[63] 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.

2.10.2 Scope

[Part 1 Coordinated preparedness testing]

The provision of preparedness support services shall include the 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 for 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, such as**:

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

The support will target the competent authorities in the Member States, 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 addresses entities operating in highly critical and other critical sectors as referred to in Annex I and II of the NIS 2 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[64] and the EU Vulnerability Database.
- 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 training courses:

- Develop[65] 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 continuous learning activities[66] to keep up with all cybersecurity requirements driven by EU cybersecurity-related regulations and directives, including the NIS 2 Directive, CSA, CSoA, DORA, EECC, GDPR, CRA.

The support will target the competent authorities in the Member States, 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)/Cyber Hubs, 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, among others, for the on boarding to the CEF Cybersecurity Core Service Platforms of public and private organisations which are working on the implementation of the NIS 2 Directive and are potential users of the CEF Cybersecurity Core Service Platforms.

---

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

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

[66] Based on ECSF: https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

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 and may support the implementation of the NIS 2 Directive.

2.10.3 Expected Outcomes

The types of deliverables are presented in two parts.

The first part covers:

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

The second part covers:

- Risk monitoring services
- Better compliance, coordinated vulnerability disclosure and monitoring
- Improved skills, via exercises and training courses, organisation of events, workshops. stakeholder consultations and white papers.

For coordinated preparedness testing:

Type of action	Simple Grant
Indicative budget	*EUR 25 million (EUR 10 million in 2025, EUR 10 million in 2026 and EUR 5 million in 2027)*
Indicative call planning	2025, 2026, 2027
Indicative duration of the action	3 years
Implementation	ECCC
Types of Beneficiaries	Public bodies acting as cybersecurity competent authorities or CSIRTs. Public bodies subject to the NIS 2 Directive, CRA, CSA, CSoA, DORA etc.
Security	Call for grants and procurement are restricted based on Article 12(5) of the DEP Regulation (2021/694).

For other preparedness actions:

Type of action	Simple Grants
Indicative budget	*EUR 15 million (EUR 5 million in 2026 and EUR 10 million in 2027)*
Indicative call planning	2026, 2027
Indicative duration of the action	3 years
Implementation	ECCC
Types of Beneficiaries	Public bodies acting as cybersecurity competent authorities or CSIRTs, National Cyber Hubs, as identified by the Member States. Public bodies and other entities subject to the NIS 2 Directive (highly critical and other critical sectors entities), CRA, CSA, CSoA, DORA etc.

	Or[67] Industry stakeholders, other public and private entities that can support the implementation of the NIS 2 Directive (along with or for highly critical and other critical sectors or entities), CRA, CSA, CSoA, DORA, GDPR, etc. Trusted cybersecurity service providers.
Security	Call for grants and procurement are restricted on the basis of Article 12(5) of the DEP Regulation (2021/694).

2.11 Mutual assistance

2.11.1 Objective

These actions aim to complement and not duplicate efforts by the Member States and those at Union level to increase the capabilities to respond to 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)(f), of Directive (EU) 2022/2555.

2.11.2 Scope

The provision of mutual assistance support shall cover technical assistance provided by one Member State to another Member States to respond to significant or large-scale cybersecurity incidents. The technical assistance may include the following activities:

- 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 State's cybersecurity competent authority, CSIRT to another Member State's competent authority for cybersecurity, CSIRT and should be to support incident response activities for significant or large-scale

[67] There should be separate calls for each type of beneficiary.

cybersecurity incidents affecting entities operating in highly critical and other critical sectors as defined in Directive (EU) 2022/2555.

The support shall be awarded directly without a call for proposals for grants[68].

In accordance with Article 196(2), second subparagraph, point (a), of Regulation (EU) 2024/2509, 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) 2024/2509, unused commitment and payment appropriations for 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 Expected Outcome

- Technical assistance to respond to significant and large-scale cybersecurity incidents.

Type of action	**Simple Grants (GRANT FOR NAMED BENEFICIARIES)**
Indicative budget	*EUR 4 million*
Indicative call planning	2026, 2027
Indicative duration of the action	3 years
Implementation	ECCC
Types 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 DEP Regulation (2021/694).

2.12 Regional Cable Hubs

As part of the EU Action Plan on Cable Security, it was announced that the Commission, together with voluntary Member States, will work on Cable Integrated Surveillance Mechanisms per sea basin ('Regional Cable Hubs') to enhance the detection capacity against threats to undersea cables as they are critical infrastructure.

Taking into account the fact that these cables are covered by the scope of NIS2 Directive that follows an all-hazards approach, it is crucial to protect their physical environment from events such as malicious acts, including cuts as integral part of the cable cybersecurity measures.

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

2.12.1 Objective

The objective is to support the progressive establishment of Regional Cable hubs, one per sea basins of the EU, whose role will be to concretely enhance threats detection and operational security around these strategic infrastructures.

This action is therefore aimed at supporting the set-up of processes, tools and services for detection and analysis of emerging threats, to establish a near real time situational awareness to protect the undersea cables. It includes the capacity to aggregate data and security information from all available sources (including established systems such as the Integrated Maritime System, or CISE, or National Cyber Hubs) and analyse them in an automated way. The action will support also the establishment of a reporting incident function and a procedure for information sharing between relevant national authorities.

Additionally, structured partnership with private sector to enhance the voluntary information sharing for cable security as well as the potential and progressive integration of the relevant defence dimension capacities – in a dual use approach – could be considered in the action.

Should the participating Member States so decide, the regional cable hubs could coordinate the deployment and activation of modular repair equipment across a sea basin.Finally, the scope could also cover the acquisition of additional capacities, equipment, tools, instruments or services useful for the enhancing the resilience and security of undersea cables.

2.12.2 Expected outcomes

The Regional cable hubs will contribute to enhancing and consolidating collective situational awareness and capabilities in detection, supporting the development of an operational capacities to ensure the security and resilience of undersea cables.

The hubs should act as a central point allowing for broader pooling of data and information relevant for the security environment of the cables, enabling the dissemination of threat information and incident detection on a regional scale and among a diverse set of national actors as designated by each Member States (e.g. National Hubs, CSIRTs.)

The Hubs should allow a rapid exchange of information, even if classified among participating authorities in a given hub. To that end, the participating authorities shall set procedural arrangements on cooperation and information sharing.

Furthermore, regional cable hubs could also benefit from additional solutions for the surveillance and protection of submarine cables, and the detection of malicious activities. For instance, situational awareness performed through the collection and analysis of in-situ, sea-based sensor data as well as relevant satellite imagery or undersea drones capacities.

The Hubs could make use of existing systems which were not developed necessarily for Cable Security, such as the Integrated Maritime Systems, the Common Information Sharing Environment (CISE), the EU Copernicus Space Programme, and the Maritime Surveillance System. (MARSUR).

The Hubs should also integrate direct cooperation with private entities, especially cable operators to increase access – in a highly secured framework - to information on ongoing and future threats and voluntary incident reporting.

The Hubs should progressively also integrate the defence dimension, as any defence capacities is likely to increase the situational awareness as well as the capacity to respond fast in case of incident against these strategic critical infrastructures. To that end, Member States can integrate in the operations of the Hubs their defence capacities (e.g. navy or surveillance system) and operational command while building on international partnerships.

To support the above activities of a Regional Cable Hub, a grant will be available to cover, among others, the preparatory activities for setting up the Regional Cable Hub, its interaction and cooperation between its members and with other stakeholders, as well as the running/operating costs involved, enabling the effective operation of the Regional Cable Hub. The grant could also be used to cover the acquisition of the infrastructures, tools and services needed to build-up the Regional Cable Hub but also to equip it with the necessary capacities to enhance the security and resilience of undersea cables, such as detection capacities.

These actions aim at creating or strengthening Regional Cable Hubs, which occupy a central role in ensuring the Security and resilience of strategic and critical infrastructures, providers of essential services such as global connectivity and power supply. As previously noted, Regional Cable Hubs will have a crucial operative role in ensuring the security of undersea cables in the Union and will handle sensitive information.

Pursuant to Article 12 of Regulation (EU) 2021/694, participation to the calls funded under this topic will be therefore subject to the restrictions of Article 12(5), as specified in Appendix 3 of this Work Programme.

Type of action	Simple Grant 70% co-funding
Indicative budget	*EUR 21 million*
Indicative call planning	2025, 2026, 2027
Indicative duration of the action	3 years
Implementation	ECCC
Types of Beneficiaries	Public entities
Security	Call for grants and procurement are restricted on the basis of Article 12(5) of the DEP Regulation (2021/694).

Additional actions for improving EU cyber resilience

Several topics are presented in this section, which are a continuation of the actions started in the 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. – which do have to comply with certain 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.

2.13 Enhancing the NCC network

2.13.1 Objective

The National Coordination Centres (NCCs) set up by the Regulation (EU) 2021/887 are designed 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, by contributing to the acquisition of 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. This could also be achieved by using Financial Support for Third Parties (FSTPs)[69]. Based on the financing received in previous years and on the different operational start dates in the Member States, this activity aims to continue providing support for NCCs.

In this regard, it is important to stress that individual NCC can choose from the list of activities and deliverables included in this topic depending on their interest and mandate. There is no obligation for NCCs to execute all actions.

This topic also considers providing support for the uptake of EU cybersecurity technologies and products, commercialisation and scale-up of the 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.

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 could contribute to cybersecurity awareness. It is becoming increasingly important to inform and educate EU citizens on 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 about cybersecurity risks and threats and to support Europe-wide actions to increase the number of students in

[69] For the use of FSTPs, the GB will prepare a dedicated procedure before the launch of the call.

cybersecurity courses, students engaged in cybersecurity research activities and 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 can open the European market for small and medium-sized enterprises would also act as a springboard into international markets. This platform will ensure the competitiveness of European cybersecurity solutions. As such, this topic could also support the EU market's growth in 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.

2.13.2 Scope

The National Coordination Centre should carry out, depending on their decision, 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 and deliver tasks supporting the implementation of the Cyber skills Academy.
- promoting, encouraging and facilitating the participation of civil society and 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 stakeholders in their application phase for projects managed by the ECCC, and in full compliance with the rules of sound financial management, especially on conflicts of interests. This should be done in close coordination with the relevant NCPs set up by the 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 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 the 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).
- supporting the scaling-up of start-ups by finding other funding to implement 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.
- Supporting the Cybersecurity Competence Community registration (on platforms such as ATLAS) and contributing to the development of suitable community management tools.

In addition, this action aims to promote safer digital behaviours, grow 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.
- Promote cybersecurity awareness, best practices, and careers in schools, universities, and community events (for instance by launching a pan-European programme where young individuals will be trained as ambassadors to promote cybersecurity.)
- Strengthen collaboration between institutions for higher education, e.g. by jointly organising 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.
- In collaboration with other entities, as needed, organise periodic cybersecurity boot camps, challenges, awareness campaigns and training courses 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 regard to the activities at national, regional and local levels, such as addressing cybersecurity in national policies on research, development and innovation in the area of 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 the DEP Regulation (2021/694).

2.13.3 Expected outcomes

Depending on the decision of each NCC, one or more of the following should be covered:

- Network of national initiatives to accelerate the cybersecurity industry and facilitate 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 including in the area of dual-use technologies
- Strengthened Cybersecurity Community to support the European Cybersecurity Industrial, Technology and Research Competence Centre; Maintained technical registration possibilities for candidates for the Cybersecurity Competence Community; Technical assistance for potential applicants for ECCC calls.
- Uptake of cybersecurity solutions.
- Strengthened cybersecurity capacities of stakeholders.
- Synergetic activities that strengthen the role of NCC.

- Centralise the many initiatives focusing on raising awareness and work together with other NCCs to support a cross European approach covering education, studies, training courses and awareness campaigns[70] ; 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 dialogue.
- Support the development of cross-over educational solutions for SMEs, for example by gamification.
- 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.
- Deliverables supporting the implementation of the Cyber skills Academy.
- Support for activities dedicated to the EU Cybersecurity Challenges.

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

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

Type of action	Simple grant
Indicative budget	*EUR 38 million*
Indicative call planning	2025, 2026, 2027
Indicative duration of the action	3-4 years
Implementation	ECCC

[70] 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.

Types 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 DEP Regulation (EU) 2021/694.

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

2.14.1 Objective

The objective of this topic is to support the European ecosystem to strengthen its cybersecurity capacities and to support the implementation of the regulatory framework in line with the Cyber Resilience Act (CRA), NIS 2 Directive, GDPR, DORA, Cybersecurity Act, specific requirements of the AI Act, etc. in a homogeneous approach. Additionally, and in alignment with the Digital education plan, which emphasises 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 to 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 depending on each sector. 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 data security and protection must be promoted during the design and development of ICT products and services.

2.14.2 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. Applications should address at least one of the eligible pieces of cybersecurity legislation but can also address more.

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 support in creating national or cross-regional expert hubs to assist with these processes. Its development should involve relevant stakeholders such as CBs, 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 harmonise and standardise the documentation and tools to be used across 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 NIS 2 (e.g. incident reporting platform) and CRA (e.g. vulnerability single reporting platform).
- Establish short-term and long-term actions to prepare professionals to properly implement the requirements of new EU regulations in entities covered by those regulations.
- Develop programmes to promote diversity and equal opportunities for all young Europeans, providing tailored onboarding programmes for youth. These programmes 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 and regional authorities to enhance cyber resilience and raise cybersecurity maturity levels through development and implementation of common methodologies.
- The design and evaluation of platforms for training programmes and tools for cross-country exchange will support these efforts. Additionally, benchmarking and assessment programmes will help optimise 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 programmes aim to strengthen Europe's cybersecurity workforce and support long-term talent development.

- Support the development of cross-border collaboration programmes, 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 facilitate information sharing and knowledge building should be provided.

Overall, this action is intended to increase collaboration between national authorities, supporting or supplementing the structures under the NIS Directive 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 the deployment of cybersecurity processes and the uptake of products and services by entities.

This action involves the creation and deployment of common tools for regulation and enforcement, including targeted security audits and incident notifications to national competent authorities to facilitate 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 facilitating and centralising the notification process for NIS 2 entities.
- At vertical level within the EU, organise or support cyber threats intelligence (CTI) unclassified information sharing in confidence between stakeholders of the given vertical.
- At EU level, enabling and organising collaboration between countries and information sharing.
- Collaborate on and implement 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[71] – 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 technology researchers, privacy-enhancing technology providers, developers of ICT products and services integrating privacy-enhancing technologies, and ICT product and services user organisations.

2.14.3 Expected Outcomes

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 the administrative burden for entities, like single entry point for incident notification.
- Establish secure communication channels allowing for cooperation and information sharing initiatives.
- Support the organisation of regular meetings/workshops to identify good practices within specific sectors or emerging areas and facilitate collaborative efforts between different sectors.
- Support the development of training courses, on the basis of the ECSF and exercises that promote capacity building and internal awareness.
- **Contribution to CR standardisation**: Training materials and training actions on cybersecurity certification for national authorities and conformity assessment bodies.

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

- **Fostering certification:** Educational and supporting 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 programmes and materials, including tools for cross-country collaboration and exchange, aimed at enhancing participants' skills and readiness for real-world threats. These programmes 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 programmes to evaluate and optimise the performance of participants in cybersecurity training programmes, ensuring continuous improvement and alignment with industry standards.
- Implement peer exchange and fellowship programmes, aimed at fostering a connected, resilient community of cybersecurity professionals across Europe. These programmes 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 programmes to support the development of pan-European teams in cybersecurity competitions. These programmes will provide access to mentorship, advanced tools, and leadership training, ensuring European teams remain competitive on the global stage. Additionally, the programmes will foster the growth of a European cybersecurity leadership pipeline, enhancing Europe's visibility and effectiveness in international cybersecurity challenges.
- Support organisations, including SMEs, in assessing the robustness, applicability and relevance of security- and privacy-enhancing technologies to be integrated in 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 assessment methodologies for the purpose of CRA compliance/requirements.
- Develop best practices or guidelines for setting-up and operating market surveillance authorities in MSs; develop awareness of CRA requirements.
- Support organisations, including SMEs, in commercialising 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 make it possible 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 cooperation in the whole privacy-enhancing technology value chain, including between researchers, providers, integrators and users, and GDPR national authorities/European supervisors.

Type of action	Simple grant
Indicative budget	*EUR 32 million*
Indicative call planning	2026, 2027
Indicative duration of the action	3 years
Implementation	ECCC
Types of Beneficiaries	All stakeholders
Security	Call restricted on the basis of Article 12(5) of the DEP Regulation (EU) 2021/694.

2.15 Dedicated action to reinforce hospitals and healthcare providers

2.15.1 Objective:

This action aims to strengthen the cybersecurity 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 EU action plan on cybersecurity in hospitals and healthcare, adopted by the Commission[72] in January 2025.

2.15.2 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 to adequately protect themselves from cyber threats.

The action will support pilot projects, which will bring together stakeholders such as regional and/or national clusters associations[73] of hospitals and healthcare providers (such as national healthcare systems, hospitals or associations of hospitals, healthcare providers and/or

[72] https://commission.europa.eu/cybersecurity-healthcare_en.

[73] 'Cluster associations' refers to any legally established group of hospitals and healthcare providers, such as 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 offering 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, among others.

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 NIS 2 Directive.

2.15.3 Expected Outcomes

- 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 minimising the impact of cyberattacks, particularly for ransomware. This also includes dedicated training courses to staff.
- Pilot cybersecurity demo installations at partner hospitals and healthcare provider 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.

2.15.4 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 entities, as well as cybersecurity service providers.

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

2.16 Dual-use technologies

2.16.1 Objectives

Dual-use technologies have emerged as a cornerstone in addressing both cybersecurity threats and broader cyber defence needs. The integration of advanced civilian and military technologies under a unified framework is critical to bolstering resilience across critical infrastructure, ensuring data security. In addition, addressing cybercrime and hybrid threats will contribute to maintaining societal stability.

Cross fertilisation and spill-over effects from synergies between the civil and defence spheres have proven to be an important driver for innovation, industrial deployment and market uptake. Such effects should also be fostered for cybersecurity and cyber defence. The results could lead to increased resilience to cyber threats and better protection of both civilian and defence critical infrastructures.

Building on Digital Europe Programme, Horizon Europe, and the European Defence Fund, the EU must prioritise collaborative pilot projects. These projects results can bridge civilian and defence sectors, fostering innovations in relevant key technologies such as quantum-safe cryptography, Zero Trust Architectures (ZTA), and AI-driven threat detection systems. Such efforts are essential to addressing emerging cyber threats while ensuring interoperability and scalability across sectors.

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 Article 6.1(f) of the DEP Regulation and Article 5.3(g) of the ECCC Regulation.

2.16.2 Scope

The objective is to enhance operational cooperation between the civil and defence spheres through the development of dual-use working prototypes, ready-to-market products and operational infrastructures related to cybersecurity technologies, applications and tools that have relevance in both civilian and defence context. Examples of domains of interest for this call topic are:

- Quantum-Safe Cryptography: Develop encryption methods resistant to quantum computing attacks. These solutions will ensure secure communication and data protection for critical civilian and military infrastructures.

- Zero Trust Architectures (ZTA): Implement ZTA frameworks to enhance endpoint security and prevent unauthorised access to critical systems. These architectures can serve both civilian applications (e.g. healthcare, finance) and defence systems.

- AI-Driven Threat Detection and Response: Deploy advanced AI tools for real-time threat detection, mitigation and response. AI can be leveraged for anomaly detection in critical networks, adaptive defence mechanisms, and predictive risk assessments. AI-driven threat detection systems can enhance the ability of stakeholders, including Law Enforcement Authorities, to analyse large datasets and identify patterns of malicious activity. These systems also enable real-time prioritisation of actionable intelligence and can support investigations across sectors. Ethical considerations, including compliance with the GDPR and AI Act, must guide their deployment.

- Cyber Ranges including Digital Twins for Cybersecurity: Use Cyber Ranges solutions and Digital Twin technology to simulate potential cyberattacks on civilian and military systems and networks. This enables proactive identification of vulnerabilities and the development of effective response strategies. This would enhance the capacities of a wide range of stakeholders, including Law Enforcement Authorities.

- Advanced SOAR Tools: Develop Security Orchestration, Automation, and Response (SOAR) platforms to streamline incident response across sectors.

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

The above domains are expected to be demonstrated and deployed for (but not limited to):

- Critical Infrastructure Protection: For example, deploy dual-use AI-driven tools to monitor and secure critical infrastructures such as undersea critical infrastructure, transportation networks, communication networks, energy grids, and healthcare systems against cyber and physical threats.
- Secure Communications: For example, utilise quantum-safe communication protocols to protect sensitive data exchanges between civilian and defence stakeholders.

- Hybrid Threat Management: For example, design systems capable of countering hybrid threats, such as GPS jamming and spoofing, cable sabotage, ransomware attacks combined with disinformation campaigns, ensuring operational continuity.
- Extension of SOC/CSIRT functionalities and operations that are compatible with military requirements. The defence community can benefit from stronger civilian detection and situational awareness capabilities developed for the protection of critical infrastructure.
- Digital Fraud and Digital Violence Prevention for Public Safety: For example, dual-use technologies for the prevention of digital fraud, disinformation and identity theft through real-time monitoring and advanced digital forensics. These solutions can enhance the ability to collect and analyse digital evidence across jurisdictions, supporting victim protection and law enforcement efforts.

Upon request from the ECCC, project consortia will participate in clustering activities to define common actions and to enhance synergies between the civilian and defence communities.

2.16.3 Expected Outcomes

- Secure Data Sharing Framework: Develop standardised and encrypted communication mechanisms to facilitate seamless data exchange between civilian and military stakeholders. These mechanisms should align with GDPR and other EU regulatory requirements.
- Early Warning Systems (EWS): Establish a European-level EWS for cyber and hybrid threats. These systems should integrate real-time monitoring tools and predictive analytics to pre-emptively identify and neutralise cyber and hybrid threats targeting critical infrastructure.
- Collaborative Training Programmes: Design joint training programmes that incorporate AI and cybersecurity scenarios for both civilian (including law enforcement) and military personnel. These programmes should address sector-specific needs and hybrid threat scenarios.
- Integrated Threat Detection Systems: Deploy unified threat detection systems leveraging AI, ZTA, and Digital Twins for cross-sectoral application, targeting current and emerging cyber and hybrid threats.
- Cross-Sector Security Standards: Develop harmonised cybersecurity standards for dual-use technologies to ensure interoperability and scalability across EU Member States and propose EU-wide frameworks for harmonising cybersecurity standards, ensuring seamless integration of civilian and military technologies.
- Stakeholder Collaboration and Integration: Facilitate partnerships among diverse stakeholders, including national authorities, SMEs, academia, and industry stakeholders to foster innovation and deployment of dual-use solutions.

Type of action	Simple grants
Indicative budget	*EUR 10 million*
Indicative call planning	2026
Indicative duration of the action	3 years
Implementation	ECCC
Types 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 DEP Regulation (2021/694).

3 Programme Support Actions

Programme support actions with a budget of EUR 9 million aim at maximising the impact of EU intervention while avoiding duplication and maximising 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 ongoing 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 the DEP and DEP implementation:
    - Events (including presidency events).
    - Support for community engagement and building.
    - Support to enhance gender balance in cybersecurity.
    - Publications.
    - Communication.
    - Studies, including mapping exercises provided in Cyber Solidarity Act.
    - Supporting the EU Cybersecurity Challenges (at EU level or supporting team Europe representatives at international level) as a way for attracting new or young talent for cybersecurity.
    - Other support measures, e.g. support for the Cyber Security Atlas.

4 Implementation

The programme involves two main modes of implementation: procurement and grants.

The different natures 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[74].

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

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 the European Commission's applicable IT governance rules[75].

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[76] 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 the deadline for the 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.

[74] http://ec.europa.eu/environment/gpp/index_en.htm (Oct. 6, 2021).
[75] To be checked if pre-approval by European Commission Information and Cybersecurity Board is needed or for compliance with the cybersecurity regulation of the new EU bodies.
[76] ECCC together with the Commission services if needed.

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)[77] 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 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 the evaluation of the 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 the implementation of the Programme. Experts are invited to apply using the mechanisms and tools provided for in the Horizon Programme[78]

[77] See Article 138 of EU Financial Regulation 2024/2509.
[78] http://ec.europa.eu/research/participants/portal/desktop/en/experts/index.html.

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 taking into consideration the 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 Programme foresees two calls: opening in Q2 and Q4, of year N and closing in Q4 year N, and Q1-Q2 year N+1. This will result in the grants being signed in Q3 year N+1 and Q1 year N+2 respectively.

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

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. For the Regional cable hubs, a funding rate of 70% has been foreseen to address the urgency of this action for the protection of strategical critical infrastructures necessary for global communications and power supply.

SME support actions

Description: Type of action primarily consisting of activities directly aiming at supporting SMEs involved in building up and deploying digital capacities. This action can also be used if SMEs need to be in the consortium and make investments to access 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 of promoting cooperation and/or 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 conflicts 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.

Procurement

Description:

Procurement is a special type of action where the main goal of the action (and thus most of the costs) consists of buying goods (equipment, infrastructure) and/or services, directly or through subcontracting tasks. Procurement is the chosen instrument whenever the results of the activity should belong to the ECCC[79]. The EU financial rules apply.

Funding rate: 100 %

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[80] (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 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

[79] According to Article 4(3)(d) of the ECCC regulation, the ECCC shall implements the objective by, *where relevant and appropriate, acquiring and operating ICT infrastructure and services where necessary to fulfil the tasks*.
[80] See Article 12(5) of the DEP Regulation.

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.

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[81]. In line with the Commission Recommendation on the cybersecurity of 5G networks of 2019[82] and the subsequent report on EU coordinated risk assessment of the cybersecurity of 5G networks of 2019[83], the EU Toolbox on 5G cybersecurity[84], the second report on Member States' progress in implementing the EU toolbox on 5G cybersecurity of 2023[85], and the related Communication on the implementation of the 5G cybersecurity toolbox of 2023[86], the Commission together with the Member States has worked to jointly identify and assess cyberthreats and security risks for 5G networks[87]. 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.

[81] 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.
[82] Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5G networks, L 88/42.
[83] NIS Cooperation Group, Report on EU coordinated risk assessment of the cybersecurity of 5G networks, 9 October 2019.
[84] NIS Cooperation Group, EU Toolbox on 5G Cybersecurity, 29 January 2020.
[85] NIS Cooperation Group, Second report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity, June 2023.
[86] Communication from the Commission: Implementation of the 5G cybersecurity Toolbox, Brussels, 15.6.2023 C(2023) 4049 final.
[87] Within the NIS framework NIS 1 + 2 [Directive - 2022/2555 - EN - EUR-Lex (europa.eu)].

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[88] and the related Communication on the implementation of the 5G cybersecurity toolbox of 2023[89].

In accordance with Article 136(2) of the Financial Regulation[90], 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 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 strategic assets and interests in question 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).

[88] NIS Cooperation Group, Second report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity, June 2023.
[89] Communication from the Commission: Implementation of the 5G cybersecurity Toolbox, Brussels, 15.6.2023 C(2023) 4049 final.
[90] 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 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 a 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 purchase, use, and 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 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 activities in question, duly described and justified for each action in the corresponding section of the WP.

Appendix 5 – Abbreviations and Acronyms

AI	Artificial Intelligence
AI/ML	Artificial Intelligence and Machine Learning
CBP	Cross-Border Platforms
CEF	Connecting Europe Facility
CERT	Computer Emergency Response Team
CRA	Cyber Resilience Act
CSA	Cybersecurity Act
CSAF	Common Security Advisory Framework
CSoA	Cyber Solidarity Act
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
DORA	Digital Operational Resilience Act
EC	European Commission
ECCC	European Cybersecurity Industrial, Technology and Research Competence Centre
ECSF	European Cybersecurity Skills Framework
EDIC	European Digital Infrastructure Consortium
EDIH	European Digital Innovation Hub
EEA	European Economic Area
EEA/EFTA	European Economic Area/European Free Trade Association countries (Iceland, Liechtenstein and Norway)
ENISA	European Union Agency for Cybersecurity
ERDF	European Regional Development Fund
ERIC	European Research Infrastructure Consortia
EUVDB	EU Vulnerability Database
GDPR	General Data Protection Regulation
IoT	Internet of Things
ISACs	Information Sharing and Analysis Centres
MCPs	Multi-Country Projects
MISP	Malware Information Sharing Platform
MS	Member States
NCCs	Network of National Coordination Centres
NIS Directive	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