DECISION No GB/2025/16

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

Amending the Single Programming Document 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 Recital (23) of the Regulation, according to which Commission Delegated Regulation (EU) 2019/7152[2] applies to the ECCC.

Having regard to Regulation (EU, Euratom) 2024/2509[3] of the European Parliament and of the Council of 23 September 2024 on the financial rules applicable to the general budget of the Union, and in particular Article 70 thereof.

Having regard to Article 30 of the ECCC Governing Board Decision No GB/204/3 on the ECCC's Financial Rules.

Having regard to the ECCC Governing Board Decision No GB/2024/13 on the adoption of the Single Programming Document (SPD) 2025-2027.

Having regard to the ECCC Governing Board Decision No GB/2025/7 on the Amendment 1 of the Single Programming Document (SPD) 2025-2027.

Whereas:

1. The SPD must be regularly updated to reflect new strategic priorities, financial resources, work programmes updates and programme synergies, particularly in the evolving field of cybersecurity.

2. The ECCC Digital Europe Programme (DEP) Cybersecurity Work Programme 2025-2027 has been amended by the Governing Board of the ECCC with ECCC GB Decision No GB/2025/15 and provides updated list of topics and budget allocations. The ECCC DEP Work Programme is hereby amended to align with the most recent policy priorities and updated budgetary allocations for 2025.

4. All these changes needed to be reflected in the SPD 2025/-2027 which is to be amended.

[1] OJ L 202, 8.6.2021, p. 1-31
[2] OJ L 122, 10.5.2019, p. 1.
[3] OJ L, 2024/2509, 26.9.2024.

HAS ADOPTED THE FOLLOWING DECISION:

Article 1

The Single Programming Document 2025-2027 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, 15 October 2025

For the European Cybersecurity
Industrial, Technology and Research
Competence Centre

(e-signed)

Pascal Steichen
Chairperson of the Governing Board

EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Single Programming Document 2025-2027

Consolidated amendment 2, Version 3, October 2025
approved by the Governing Board of the ECCC Decision No GB/2025/16

DOCUMENT HYSTORY

No	Version	Comment
1	Decision No GB/2024/13	Adopted in December 2025
2	Amendment 1, Decision No GB/2025/7	Updated following the adoption of HE WP 2025 and allocation of budget for ECCC implementation.
3	Amendment 2, Decision No GB/2025/16	Incorporates the reduction of revenue due to amendment 2 of DEP Cybersecurity WP 2025-2027, adopted by ECCC GB Decision No GB/2025/15.

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

COPYRIGHT NOTICE

TABLE OF CONTENT

FOREWORD

The European Cybersecurity Competence Centre (ECCC) was established to enhance cybersecurity capabilities in the EU and to support better coordination amongst relevant stakeholders to achieve common goals of EU citizens, society and economy. Whilst in 2024 the ECCC reached its financial autonomy, moved to the permanent premises and took over running Horizon Europe and Digital Europe programmes (HEP, DEP) projects on cybersecurity, 2025 will be the year when the last element of the governance will be finalised with the registration of members to the Cybersecurity Competence Community (the Community) and the appointment of the member of the Strategic Advisory Group.

During 2025, the ECCC will be on cruising speed, fully operational, coordinating and managing calls under the HEP and DEP, coordinating the set-up of the Cyber Hubs and fostering cooperation of the Cybersecurity Competence Community.

The activities of the ECCC are part of a bigger picture at EU level. In recent years, the EU has continued developing its cybersecurity policy. This includes the NIS 2 Directive, as well as more recent legislative initiative such as the Cyber Resilience Act and the Cyber Solidarity Act, on which the co-legislator reached political agreement, and which are now undergoing final adoption stages. It also includes the Communications on the Cybersecurity Skills Academy and on cyber defence, as well as funding calls for proposals launched in 2022 and 2023 under the HEP and DEP, amongst other initiatives.

The ECCC, together with the National Coordination Centres (NCCs) are an important component of this coordinated effort to enhance cybersecurity capabilities and improve resilience in the EU. The ECCC Regulation, which entered into force in mid-2021, aims to improve cyber capabilities in the EU, inter alia, in terms of scientific and industrial assets, specialised competences and general cyber awareness, and to improve coordination amongst relevant stakeholders. This implies setting strategic objectives for investment, deployment, and use of cybersecurity products and services, pooling resources from the EU, notably from the DEP, Member States and other players.

The present document provides an updated multiannual planning 2025-2027 and work programme for 2025, following consultations with the ECCC GB. The document is in line with the Strategic Agenda of the ECCC adopted by the ECCC GB in March 2023 and proposes actions to monitor its implementation. It follows the guidelines from the Commission Communication on the strengthening of the governance of Union Bodies, under Article 70 of the Financial Regulation 2018/1046, and on the guidelines for the Single Programming Document and the Consolidated Annual Activity Report.

In 2025 the ECCC shall function as an autonomous EU body, with an Executive Director formally appointed and with all staff recruited. By then, the ECCC will capitalise on the results of the hard work from previous years and the engagement of all those that contributed to the set-up of the ECCC, including ECCC staff, European Commission (EC) staff working on the ECCC, the Network of NCCs and many in the Cyber Competence Community. The vision from the ECCC regulation will increasingly materialise, showing the added value of the EU strategic investments and enhanced coordination on cybersecurity.

Note on the amendment 1: This document includes the amendments required to provide more information (1) on the final adopted ECCC Work Programme for 2025-2027 implementing the cybersecurity parts of the Digital Europe Programme (in particular actions related to Article 6 of Regulation (EU) 2021/694) adopted by the ECCC GB in March 2025[1] (and amended in June 2025[2]) and (2) on the Horizon Europe Programme 2025 adopted by the Commission in

[1] Decision 2025/04 of the GB, available from here: https://cybersecurity-centre.europa.eu/governing-board_en
[2] Decision 2025/6 of the GB, available from here: https://cybersecurity-centre.europa.eu/governing-board_en

May 2025[3], whereby Commission intends to conclude a contribution agreement with the European Cybersecurity Competence Centre (ECCC) for the implementation of Horizon Europe cybersecurity actions not co-funded by Member States, in accordance with Article 5(5) of Regulation (EU) 2021/887, and in particular for the implementation of call topics related to Increased Cybersecurity in accordance with the Horizon Europe. The sections dedicated to 2025 implementation and related budgets are updated to reflect these changes.

June 2025

Luca TAGLIARETTI

Executive Director

[3] Horizon Europe Programme for 2025, available at: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2025/wp-6-civil-security-for-society_horizon-2025_en.pdf

LIST OF ACRONYMS

ABAC	Accrual-based accounting
AD	Administrator
AST	Assistant
BOA	Back Office Arrangements
CA	Contract agent
CERT-EU	Computer Emergency Response Team for the EU institutions, bodies and agencies
CRA	Cyber Resilience Act
CSA	Cybersecurity Act
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
DEP	Digital Europe Programme
DPO	Data Protection Officer
EC	European Commission
ECA	European Court of Auditors
ECCC	European Cybersecurity Competence Centre
ECSO	European Cyber Security Organisation
ED	Executive Director
EFTA	European Free Trade Association
EIB	European Investment Bank
ENISA	European Union Agency for Cybersecurity
EU	European Union
EUAN	EU Agencies Network
EU-LISA	European Union Agency for the Operational Management of Large-scale IT Systems in the Area of Freedom, Security and Justice
Europol	European Union Agency for Law Enforcement Cooperation
FTE	Full-time equivalent
GB	Governing Board (of the ECCC)
HEP	Horizon Europe Programme
ICT	Information and communication technology
ISAC	Information Sharing and Analysis Centre
IT	Information technology
JCU	Joint Cyber Unit
JU	Joint Undertaking
MoU	Memorandum of understanding
MS	Member State(s)
NCCs	National Coordination Centres
NIS	Networks and information systems
NIS CG	NIS Cooperation Group
NLO	National Liaison Officers
SAG	Strategic Advisory Group
SC	Secretary
SLA	Service-level agreement
SMEs	Small and medium-sized enterprises
SOP	Standard Operating Procedure
SPD	Single Programming Document
TA	Temporary agent
TESTA	Trans European Services for Telematics between Administrations
TFEU	Treaty on the Functioning of the European Union

MISSION STATEMENT

The European Cybersecurity Competence Centre (ECCC)[4] is a European Union (EU) body established by Regulation (EU) 2021/887[5] of the European Parliament and of the Council ("the Regulation"), which entered into force on 28 June 2021.

The Regulation provides the ECCC with the mandate to support industrial technologies, research and innovation in the domain of cybersecurity, collaborating with the Network of National Coordination Centres (NCCs) and stakeholders from the Cybersecurity Competence Community (the Community). The ECCC manages EU financial resources dedicated to cybersecurity under the Digital Europe Program (DEP)[6] and the Horizon Europe Program (HEP)[7], and other EU programmes where appropriate, as well as additional contributions from Member States, to implement projects and initiatives on cybersecurity research, technology and industrial development. The ECCC has adopted an Agenda[8] for cybersecurity development and deployment, which pays particular attention to small and medium-sized enterprises (SMEs). The ECCC and the Network of NCCs contribute to Europe's technological sovereignty and open strategic autonomy through joint investment in strategic cybersecurity projects. More concretely, according to Article 3 of the Regulation, the ECCC and the Network of NCCs have the mission to help the EU to:

- Strengthen its leadership and strategic autonomy in the area of cybersecurity by developing the EU's research, technological and industrial cybersecurity capacities and capabilities necessary to enhance trust and security, including the confidentiality, integrity and accessibility of data in the Digital Single Market.
- Support the EU technological capacities, capabilities and skills in relation to the resilience and reliability of the infrastructure of network and information systems, including critical infrastructure and commonly used hardware and software; and
- Increase the global competitiveness of the EU's cybersecurity industry, ensure high cybersecurity standards throughout the EU and turn cybersecurity into a competitive advantage for other EU industries.

According to Article 4 the Regulation, the ECCC shall have the overall objective of promoting research, innovation and deployment in the area of cybersecurity. Beyond its overall objective, the ECCC has the following specific objectives:

- Enhancing cybersecurity capacities, capabilities, knowledge and infrastructure for the benefit of industry, in particular SMEs, research communities, the public sector and civil society.

[4] https://cybersecurity-centre.europa.eu/index_en.
[5] Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (OJ L 202, 8.6.2021, p. 1).
[6] Digital Europe Programme established by Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 (OJ L 166, 11.5.2021, p. 1).
[7] Horizon Europe Programme established by Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013 (OJ L 170, 12.5.2021, p. 1).
[8] Such Agenda is foreseen by the ECCC regulation. The ECCC Strategic Agenda, adopted by ECCC GB in March 2023 is available at: https://cybersecurity-centre.europa.eu/strategic-agenda_en

- Promoting cybersecurity resilience, the uptake of cybersecurity best practices, the principle of security by design, and the certification of the security of digital products and services, in a manner that complements the efforts of other public and private entities; and
- Contributing to a strong European cybersecurity ecosystem bringing together all relevant stakeholders.

With a view to achieving those objectives, the ECCC shall:

- Establish strategic recommendations for research, innovation and deployment in cybersecurity, in accordance with EU legislation and policy orientations, and set out strategic priorities for the ECCC's activities.
- Implement actions under relevant EU funding programmes, in accordance with the relevant work programmes and the EU legislative acts establishing those funding programmes.
- Foster cooperation and coordination among the NCCs and with and within the Community; and
- Where relevant and appropriate, acquire and operate the Information and Communication Technologies (ICT) infrastructure and services required to fulfil its tasks.

With regards to the ECCC's tasks, according to Article 5 of the Regulation:

- The ECCC supported by the Network will make strategic investment decisions and pool resources from the EU, its Member States (MS) and, indirectly, other cyber constituencies, to improve and strengthen technology and industrial cybersecurity capacities, enhancing the EU's open strategic autonomy.
- The ECCC will play a key role in delivering on the ambitious cybersecurity objectives of the DEP and HEP.
- The ECCC together with the Network will support the deployment of innovative cybersecurity solutions in the Community and beyond.
- It will also facilitate collaboration and coordination and the sharing of expertise between relevant stakeholders from the Cybersecurity Competence Community, in particular research and industrial communities, as well as NCCs.

SECTION I. GENERAL CONTEXT

The "*EU's Cybersecurity Strategy for the Digital Decade*"[9] outlines the EU vision and plan for cybersecurity. Building upon previous achievements, the strategy contains concrete proposals for regulatory, investment and policy initiatives, in three areas of EU action:

- "Resilience, technological sovereignty and leadership", aiming to protect EU people, businesses and institutions from cyber incidents and threats.
- "Building operational capacity to prevent, deter and respond", aiming to enhance the trust of individuals and organisations in the EU's ability to promote secure and reliable network and information systems, infrastructure and connectivity; and
- "Advancing a global and open cyberspace through increased cooperation", aiming to promote and protect a global, open, free, stable and secure cyberspace grounded in human rights, fundamental freedoms, democracy and the rule of law.

As stated in the Council conclusions on the Joint Communication to the European Parliament and the Council entitled "*The EU's Cybersecurity Strategy for the Digital Decade*"[10], achieving strategic autonomy while preserving an open economy is a key objective of the EU in order to self-determine its own economic path and interests. This includes reinforcing the ability to make autonomous choices in the area of cybersecurity with the aim to strengthen the EU's digital leadership and strategic capacities. Furthermore, it can also include diversifying production and supply chains, fostering and attracting investments and production in Europe, exploring alternative solutions and circular models, and promoting broad industrial cooperation across MS. The conclusions also acknowledge the importance of continued support for technical assistance and cooperation between MS for capacity-building purposes.

As highlighted in the Nevers Call[11], Russia's invasion of Ukraine and its repercussions in the cyber-space has reinforced the case for strengthening cooperation in cyber crisis management at EU level. The Cyber Posture Council Conclusions[12] notably call on the EC, the High Representative of the Union for Foreign Affairs and Security Policy, and MS to carry out a risk evaluation and develop risk scenarios from a cybersecurity perspective in a situation of threat or possible attack against Member States or partner countries.

Such an initiative echoes the EU's ambition for a common situational awareness and coordinated preparation and response to threats. A key priority area on which efforts are focusing is the development of shared situational awareness. This includes stronger inter-agency cooperation among ENISA, CERT-EU and Europol in assessing the threat landscape while working closely with the EU MS and networks (i.e. EU-CyCLONe, CSIRTs network, NIS Cooperation Group). Moreover, the political agreement on the NIS 2 Directive[13] provides a legal basis for the EU-CyCLONe, the network of MS cyber crisis management authorities plus, in case of potential or ongoing large-scale

[9] Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade, JOIN/2020/18 final.
[10] Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade (6722/21).
[11] 'Nevers Call to Reinforce the EU's Cybersecurity Capabilities'. Informal Meeting of the Telecommunications Ministers. Nevers, March 9, 2022.
[12] https://www.consilium.europa.eu/en/press/press-releases/2022/05/23/cyber-posture-council-approves-conclusions/
[13] Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM/2020/823 final.

cybersecurity incident[14] has or is likely to have a significant impact on services and activities falling within the scope of the NIS 2 Directive, the EC, to participate in crisis management coordination and situational awareness.

The establishment of the ECCC is taking place in a dynamic cybersecurity political context, including several initiatives at EU level:

- Revision of the NIS Directive (NIS2). To respond to the increased exposure of Europe to cyber threats, the EC proposed, in December 2020, a revision of the NIS Directive (NIS 2 Directive). The Directive was adopted in December 2022, and the national transposition measures shall be applied as from 18 October 2024. The new Directive raises the EU common level of ambition on cyber-security, through a wider scope, clearer rules and stronger supervision tools.
- Cybersecurity Resilience Act (CRA). In September 2022, the EC adopted the proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act, CRA)[15]. The CRA establishes a horizontal legal framework for cybersecurity essential requirements for placing products with digital elements on the market. The CRA aims to ensure that hardware and software products are placed on the EU market with fewer vulnerabilities and that manufacturers take cybersecurity seriously throughout the whole product lifecycle. It also aims to create conditions that allow users to take cybersecurity into account when selecting and using products with digital elements. On 30 November 2023, the co-legislators have agreed on a political compromise text for the legislative proposal and the Cyber Resilience Act is expected to enter into force in the course of 2024.
- Cyber Solidarity Act. In April 2023, the Commission adopted a proposal for a Cyber Solidarity Act, including amendments to Digital Europe Programme Regulation, designed to: (1) strengthen common coordinated Union detection capacities and common situational awareness of cyber threats and incidents; (2) reinforce preparedness and enhance response and recovery capacities to handle significant, large-scale and large-scale equivalent cybersecurity incidents; (3) enhance union resilience and contribute to effective response by reviewing and assessing significant or large-scale incidents. The Cyber Solidarity Act will complement ECCC actions to provide long-term solutions to strengthen solidarity at Union level. On 6 March 2024, the co-legislators have agreed on a political compromise text for the legislative proposal and the Cyber Solidarity Act is expected to enter into force in the course of 2024. The Cyber Solidarity Act provides for a number of actions for the ECCC to implement. The ECCC will be responsible for actions related to the European Cybersecurity Alert System, including managing the joint procurement with Member States of tools, infrastructures and services needed for the Cyber Hubs, the accompanying grants and conducting the mapping of the tools, infrastructures and services necessary to establish or enhance National Cyber Hubs and Cross-Border Cyber Hubs. The ECCC will also be responsible under the Cybersecurity Emergency Mechanism for managing the calls for grants for the preparedness actions, including coordinated preparedness testing and other preparedness actions and managing the support within the mutual assistance action.
- Measures for a high common level of cybersecurity for EU institutions, bodies, offices and agencies. The EC presented a proposal for a regulation to enhance the cybersecurity and information security of the EU institutions, bodies, offices and agencies, which entered into force in December 2023. The 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 inter-institutional Cybersecurity Board to monitor the Regulation's implementation.

[14] See please NIS 2 Directive, Article 16(2)
[15] Proposal for Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM/2022/454 final.

- European Cybersecurity certification schemes. The European Cybersecurity Certification Framework laid out in the Cybersecurity Act[16] aims at creating market-driven European cybersecurity certification schemes and increasing "cybersecurity-by-design" in ICT products, services, and processes. 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 such as the development of harmonised evaluation methodologies or innovations to the performance of testing ICT products, services and processes.
- EU 5G Toolbox. The EU 5G Toolbox[17] is a comprehensive and objective risk-based approach for the security of 5G and future generations of networks. In June 2023, the NIS Cooperation Group adopted a report on the status of implementation of the EU 5G Toolbox[18], which showed that a vast majority of Member States have reinforced or are in the process of reinforcing security requirements for 5G networks based on the EU Toolbox, but some of the key measures have not been fully implemented yet in all Member States. The EC also adopted a Communication on this topic at the same time[19], in which it underlined its strong concerns about the risks to EU security posed by certain 5G suppliers and committed to ensure that its own corporate communications and Union funding activities will not rely on these suppliers. In addition, the NIS Cooperation Group, with the support of the EC and ENISA, carried out a risk assessment on the telecommunications sector[20] at large and identified a number of key threats that could pose significant risks for the security and resilience of the connectivity infrastructure. To mitigate these risks, a number of strategic and technical recommendations for Member States, the Commission and ENISA, are put forward.
- EU funding in the 2021-2027 Multiannual Financial Framework. In 2022 and 2023 funding was provided for projects on cybersecurity deployment under the DEP, and for cybersecurity research under the HEP, while further funding is foreseen under both EU programs. The respective work programmes 2023-2024, including support for cybersecurity, were adopted in 2023.
- EU Cybersecurity Skills Academy. In 2023 the EC adopted a non-legislative initiative outlining policy and support measures to promote cyber skills.
- EU Cyber Defence Policy. It was endorsed by Council Conclusions in 2023[21] and it includes references to the ECCC as an essential pillar to support the scale up of European cybersecurity industry.

Within this broad framework of EU cybersecurity policy priorities, the ECCC will pool resources from the EU, MS and other constituencies to improve and strengthen technological and industrial cybersecurity capacities, enhancing the EU's open strategic autonomy, and offering a possibility to consolidate part of the cybersecurity-related activities funded under HEP and DEP.

[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.
[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

The ECCC and the Network of NCCs and the Community will contribute to maximising the effects of investments to strengthen the EU's leadership and open strategic autonomy in the field of cybersecurity and support technological capacities, capabilities and skills, and to increase the EU's global competitiveness. They will do so with input from industry and academic communities in cybersecurity, including SMEs and research centres, through a more systematic, inclusive and strategic collaboration.

Furthermore, the ECCC shall cooperate with relevant EU institutions, bodies, offices and agencies, in particular with ENISA, in order to ensure consistency and complementarity while avoiding any duplication of effort.

Note on the amendment 1: This document includes the amendments required to provide more information (1) on the final adopted ECCC Work Programme for 2025-2027 implementing the cybersecurity parts of the Digital Europe Programme (in particular actions related to Article 6 of Regulation (EU) 2021/694) adopted by the ECCC GB in March 2025[22] (and amended in June 2025[23]) and (2) on the Horizon Europe Programme 2025adopted by the Commission in May 2025[24], whereby Commission intends to conclude a contribution agreement with the European Cybersecurity Competence Centre (ECCC) for the implementation of Horizon Europe cybersecurity actions not co-funded by Member States, in accordance with Article 5(5) of Regulation (EU) 2021/887, and in particular for the implementation of call topics related to Increased Cybersecurity in accordance with the Horizon Europe. The sections dedicated to 2025 implementation and related budgets are updated to reflect these changes.

[22] Decision 2025/04 of the GB, available from here: https://cybersecurity-centre.europa.eu/governing-board_en
[23] Decision 2025/6 of the GB, available from here: https://cybersecurity-centre.europa.eu/governing-board_en
[24] Horizon Europe Programme for 2025, available at: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2025/wp-6-civil-security-for-society_horizon-2025_en.pdf

SECTION II. MULTI-ANNUAL PROGRAMMING 2025 – 2027

The ECCC, in consultation with its GB, developed a multi-annual programming covering three years. Compared to the initial years of operation of the ECCC, this multiannual programming introduces a shift in focus given the maturity level reached by the ECCC. During the first years, following the establishment of ECCC, one of the main objectives was to make the ECCC operational, develop its financial and operational autonomy, and gradually deliver all it's the core tasks. For 2025 and the following years, the focus shifts to the core ECCC tasks: the implementation of programmes and fostering communities.

Article 4(3) of ECCC regulation presents the way ECCC should implements its specific operational objectives, by:

> *(a) establishing strategic recommendations for research, innovation and deployment in cybersecurity in accordance with Union law and setting out strategic priorities for the Competence Centre's activities.*
>
> *(b) implementing actions under relevant Union funding programmes in accordance with the relevant work programmes and the Union legislative acts establishing those funding programmes.*
>
> *(c) fostering cooperation and coordination among the national coordination centres and with and within the Community; and*
>
> *(d) where relevant and appropriate, acquiring and operating ICT infrastructure and services where necessary […].*

This multiannual work programme of the ECCC is aligned with Article 4(3), comprising three activities: Activity 1, corresponding to paragraphs (b) and (d), and Activity 2, corresponding to paragraph (a) and (c) of Article 4(3) of the ECCC Regulation. One more horizontal/cross cutting activity: Activity 3, to support the functioning of the ECCC and its staff. As such the following activities are presented in this document:

- *Activity 1 – Deployment of resources for cybersecurity*, dedicated to implementing actions under relevant Union funding programmes; and where relevant acquiring and operating ICT infrastructure and services to fulfil the tasks set out in Article 5 of the ECCC regulation.
- *Activity 2 – Strategic advice, cooperation and coordination for cybersecurity*, dedicated to the NCCs and the Community, and also establishing strategic recommendations for research, innovation and deployment in cybersecurity, as well as priorities for the ECCC's activities.
- *Activity 3 – Governance, establishment and compliance of the ECCC*, dedicated to the operation of the ECCC, its financial and human resources, IT and infrastructures, legal and compliance related activities.

The proposed activities are in line with the activities in previous SPDs, with some differences: new Activity 1 corresponds to Activity 2 in previous SPDs; new Activity 2 corresponds to Activities 3 and 4 in previous SPDs; Activity 3 corresponds to Activity 1 in previous SPDs.

The next table lists the ECCC responsibilities under its founding Regulation and their correspondence to the referred 3 activities.

ECCC tasks and responsibilities	Activity 1	Activity 2	Activity 3
Article 5 - Tasks of the Competence Centre			
1.(a) strategic tasks (as detailed in paragraph 2 and listed below), consist of			
2.(a) developing and monitoring the implementation of the Agenda		√	√
2.(b) through the Agenda and the multiannual work programme, while avoiding any duplication of activities with ENISA and taking into account the need to create synergies between cybersecurity and other parts of Horizon Europe and the Digital Europe Programme		√	
2.(c) ensuring synergies between and cooperation with relevant Union institutions, bodies, offices and agencies, in particular ENISA, while avoiding any duplication of activities with those Union institutions, bodies, offices and agencies		√	√
2.(d) coordinating national coordination centres through the Network and ensuring a regular exchange of expertise		√	√
2.(e) providing expert cybersecurity industrial, technology and research advice to Member States at their request, including with regard to the procurement and deployment of technologies	√	√	
2.(f) facilitating collaboration and the sharing of expertise among all relevant stakeholders, in particular members of the Community		√	√
2.(g) attending Union, national and international conferences, fairs and forums related to the mission, objectives and tasks of the Competence Centre with the aim of sharing views and exchanging relevant best practices with other participants		√	
2.(h) facilitating the use of results from research and innovation projects in actions related to the development of cybersecurity products, services and processes, while seeking to avoid the fragmentation and duplication of efforts and replicating good cybersecurity practices and cybersecurity products, services and processes, in particular those developed by SMEs and those using open source software		√	
1.(b) implementation tasks (as detailed in paragraph 3 and listed below), consist of			
3.(a) coordinating and administrating the work of the Network and the Community in order to fulfil the mission set out in Article 3, in particular by supporting cybersecurity start-ups, SMEs, microenterprises, associations and civic technology projects in the Union and facilitating their access to expertise, funding, investment and markets		√	
3.(b) establishing and implementing the annual work programme, in accordance with the Agenda and the multiannual work programme	√	√	√
3.(c) supporting, where appropriate, the achievement of Specific Objective 4 – 'Advanced Digital Skills' as set out in Article 7 of Regulation (EU) 2021/694, in cooperation with European Digital Innovation Hubs	√	√	
3.(d) providing expert advice on cybersecurity industry, technology and research to the Commission when the Commission prepares draft work programmes pursuant to Article 13 of Decision (EU) 2021/764		√	
3.(e) carrying out or enabling the deployment of ICT infrastructure and facilitating the acquisition of such infrastructure, for the benefit of society, industry and the public sector, at the request of Member States, research communities and operators of essential services, by means of, inter alia, contributions from Member States and Union funding for joint actions, in accordance with the Agenda, the annual work programme and the multiannual work programme	√		
3.(f) raising awareness of the mission of the Competence Centre and the Network and of the objectives and tasks of the Competence Centre		√	√
3.(g) without prejudice to the civilian nature of projects to be financed from Horizon Europe, and in accordance with Regulations (EU) 2021/695 and (EU) 2021/694, enhancing synergies and coordination between the cybersecurity civilian and defence spheres		√	
Article 10 - Cooperation of the Competence Centre with other Union institutions, bodies, offices and agencies and international organisations		√	√

II.1 MULTI-ANNUAL WORK PROGRAMME

The Activities for the Multiannual Work Programme 2025-2027 of the ECCC correspond to three specific objectives, which are re-ordered and updated compared with SPD 2024-2026:

- Objective #1: Implement DEP, HEP, and as relevant other funding mechanisms, and support acquisitions

  For this Work Programme, the main funding sources foreseen will continue to come from DEP. The estimated budget for the Cybersecurity part of DEP during the 4-year period 2024-27 is approximately EUR 500 million.

  The adoption of the *ECCC Work Programme 2025-2027 implementing the cybersecurity parts of the Digital Europe Programme (in particular actions related to Article 6 of Regulation (EU) 2021/694)* is a major milestone during this period. Key tasks will be the evaluation of DEP calls, preparation and signature of grants and procurements, and managing projects. The ECCC will entirely manage these tasks, independently from EC services after reaching

full financial autonomy. In addition, the Cyber Solidarity Act provides for a series of actions to be managed by the ECCC. Furthermore, in line with Article 5.5 of the ECCC Regulation, the EC may delegate to the ECCC the implementation of HEP in the area of cybersecurity (evaluation of proposals, management of grants, etc.).

- Objective #2: Coordinate and further develop the Network of NCCs and the Cybersecurity Competence Community; develop, implement and monitor the ECCC strategic advice and priorities under the Agenda, the multiannual and the annual work programme

The ECCC will facilitate and coordinate the work of the Network of NCCs, by facilitating the works of the ECCC GB Working Groups and its Chairs as secretariat. The Network is composed of one NCC from each MS[25]. Over the course of 2022, seven Working Groups (WGs) of the GB were established, of which several relate to the functioning of the NCCs Network. During 2024 the WG were revised, and the following list reflects latest agreement of the ECCC GB during the meeting in June:

- WG1: Community Building
- WG 2: Boost application process success
- WG 3: International awareness
- WG 4: Strategic advice
- WG 5: Cyber skills
- WG 6: Cyber Hubs

Articles 18-20 of the ECCC Regulation foresee a Strategic Advisory Group (SAG) that will regularly advise the ECCC in respect of the performance of its activities and ensure communication with the Community and other relevant stakeholders. The SAG could be established once a critical mass and regional balance of community members will be identified. The Community, in particular through the SAG, should provide input to the activities of the ECCC, to the Strategic Agenda, to the multiannual work programme and to the annual work programme.

The Strategic Agenda[26] of the ECCC, adopted by the GB in 2023 based on input from a dedicated Working Group of the GB, is a comprehensive strategy which sets out priorities for the development of European cybersecurity capabilities and for ECCC's activities[27], according to the following high-level structure:

1. To support SMEs to develop and use strategic cybersecurity technologies, services and processes:
   1.1 Processes and tools for managing cybersecurity information and risk management
   1.2 Secure and resilient hardware and software systems
2. To support and grow the professional workforce:
   2.1 Development of cybersecurity skills: education and professional training
   2.2 Cybersecurity skills framework and competence assessment
3. To strengthen research, development and innovation expertise in the broader European cybersecurity ecosystem:
   3.1 Promoting post-quantum cryptography standardisation and adoption
   3.2 Support for European Cybersecurity Certification
   3.3 Strengthening market competitiveness
   3.4 Promoting collaboration and information sharing

The Strategic Agenda includes also short-term impact statements (2023-2027):

[25] NCCs are upon their request, in accordance with Article 6(2) or 6(5) of Regulation (EU) 2021/887, assessed by the Commission as to their capacity to manage EU funds to fulfil the mission and objectives laid down in the ECCC Regulation. Further to the Commission assessment, NCCs may receive direct EU financial support, including grants awarded without a call for proposals, in order to carry out their activities. The modalities for the EU financial support to NCCs (funding amounts, call dates and other details) are indicated in the DEP work programme.
[26] The Strategic Agenda adopted by ECCC GB in March 2023 is detailed in an Action Plan endorsed by the Governing Board as a Working Document, on March 2024, not for publication.
[27] Article 2 point (8) of the Regulation

- *By 2027, the ECCC and the Network will have funded European SMEs in developing and using strategic cybersecurity technologies, services and processes through a coordinated cascade funding mechanism via NCCs and national co-financing that lowers the application threshold for SMEs.*
- *By 2027, the ECCC and the Network will have supported and grown the cybersecurity professional workforce in both quantity and quality through the standardisation and certification of cybersecurity skills and investments in education and training of cybersecurity professionals.*
- *By 2027, the ECCC and the Network will have strengthened the research, development and innovation expertise and competitiveness of the EU cybersecurity community through the development and implementation of an efficient and coherent action plan.*

When drafting the annual work programme and the multiannual work programme, the ECCC will take into account the input received from the NCCs, the Community and its working groups, the Strategic Advisory Group (SAG) (once established), the European Commission and ENISA. The GB will monitor the implementation and ensure the dissemination of the Strategic Agenda and its update.

The Strategic Agenda will guide the drafting of the annual and multiannual work programmes of the ECCC, more specifically for Activity 1.

The annual work programme of the ECCC will define, in accordance with the Strategic Agenda and the multiannual work programme, the cyber priorities for the DEP and, to the extent that they are co-financed by the MS, also the priorities for the HEP, in line with article 13.3.c and 21.3.b of the ECCC Regulation The HEP and DEP work programmes may include "joint actions" between the ECCC and MS, as defined in article 2(5) of the ECCC Regulation.

- Objective #3: Consolidate financial and operational autonomy

Activities covered under this objective were predominant in previous SPDs of the ECCC, during the establishment stage. From 2025, when the ECCC will be at cruising speed, the focus is to ensure an efficient and effective management of resources, including:

- Governance, coordination and compliance
  - ED office, coordination and management of the ECCC
  - Planning and programming activities and documents
  - Relation with GB and ECCC stakeholders, including host country; Secretariat for ECCC GB
  - Liaison activities with other EU bodies in the remit of ECCC mandate
  - Compliance and internal control
  - Communication, dissemination and outreach
- Management of assets and of financial and human resources
  - Consolidate financial and human resources
  - Consolidate IT tools, ICT assets, security rules and other logistical aspects
  - Building and facilities management, including environmental management
  - Relations with host country and adequate implementation of the Host Agreement
  - Monitoring, evaluations, access to documents, reporting

II.2 HUMAN AND FINANCIAL RESOURCES - OUTLOOK FOR YEARS 2025 – 2027

II.2.1 Overview of the past and current situation

The ECCC Regulation entered into force on 28 June 2021. Since then, DG CONNECT of the EC has been working on the establishment of the ECCC. Preparatory actions, notably HR-related rules, were adopted in 2022 which enabled

the recruitment of the majority of ECCC staff members during 2023. The EC services continue acting on behalf of the ECCC until the ECCC reached full financial autonomy.

II.2.2 Outlook for the years 2025 – 2027

As of 2025, the management of DEP and HEP funding will be the focus of ECCC. Support for activities related to strategic advice, cooperation and coordination for cybersecurity, including the support for ECCC Working Groups and support for the functioning of the NCC Network and its tasks (particularly the registration process) will be taken into consideration for the human and financial resources planning.

Selection and recruitment of the initial staff members of the ECCC which started in 2022, increased significantly in 2023 and reached full capacity in 2024, including the appointment of the ED. To improve synergies and efficiency gains, the Accounting Officer and Data Protection Officer are shared with ENISA since 2023 (see section below on synergies).

II.2.3 Resource programming for the years 2025 – 2027

Financial Resources

As defined in the Regulation, the ECCC is funded by the EU, with the possibility of joint actions funded by the EU and by voluntary contributions from MS.

The EU contribution shall be paid from the appropriations in the EU general budget allocated to Cybersecurity activities in the DEP Programme, the specific programme implementing HEP established by Decision (EU) 2021/764 and other relevant EU programmes, as needed for the implementation of the tasks or the achievement of the objectives of the ECCC, subject to decisions taken in accordance with the legal acts of the EU establishing those programmes. The amounts from the table below cover all appropriations from the EU contribution / EU subsidy and from the revenue stemming from the implementation of the Horizon Europe Programme through the signature of a Contribution Agreement. For further details please see Annex III.

Table 1. Appropriations

Year	2024	2025	2026	2027
Total appropriations for ECCC (EUR)	315,326.224.22	238,868,581.55	126,099,400.49	120,392,197.49

Human Resources

The Staff Regulations and Conditions of Employment of Other Servants of the EU apply to the staff of the ECCC. The first recruitments were initiated in 2022, and continued in 2023, including the selection of the ED. Before 2025 all posts are expected to be filled, and no new posts are foreseen for 2025-2027. 2023 recruits started to work at the temporary ECCC headquarters in Bucharest, until the final move to permanent offices (in different floors of the same building) in 2024. For further info please see Annex IV.

II.2.4 Strategy for achieving efficiency gains

On July 2022, the ECCC became an ad hoc member of the EU Agencies Network (EUAN), of which full membership requires financial autonomy, thus gaining access to exchange knowledge and best practices on horizontal issues for EU agencies and bodies.

In 2023 the ECCC and ENISA signed a service-level agreement (SLA) regarding shared services (namely Data Protection Officer and Accounting Officer services). During 2024 additional SLAs have been concluded with EU bodies and

institutions, supporting this was access to services for both operational and administrative activities. The list of SLAs is presented in the annex XI.

The ECCC will look for consolidation and new ways to cooperate with other EU bodies and agencies to benefit or take inspiration from already existing resources and approaches, e.g. use of existing framework contracts for procurement.

II.2.5 Negative priorities/decrease of existing tasks

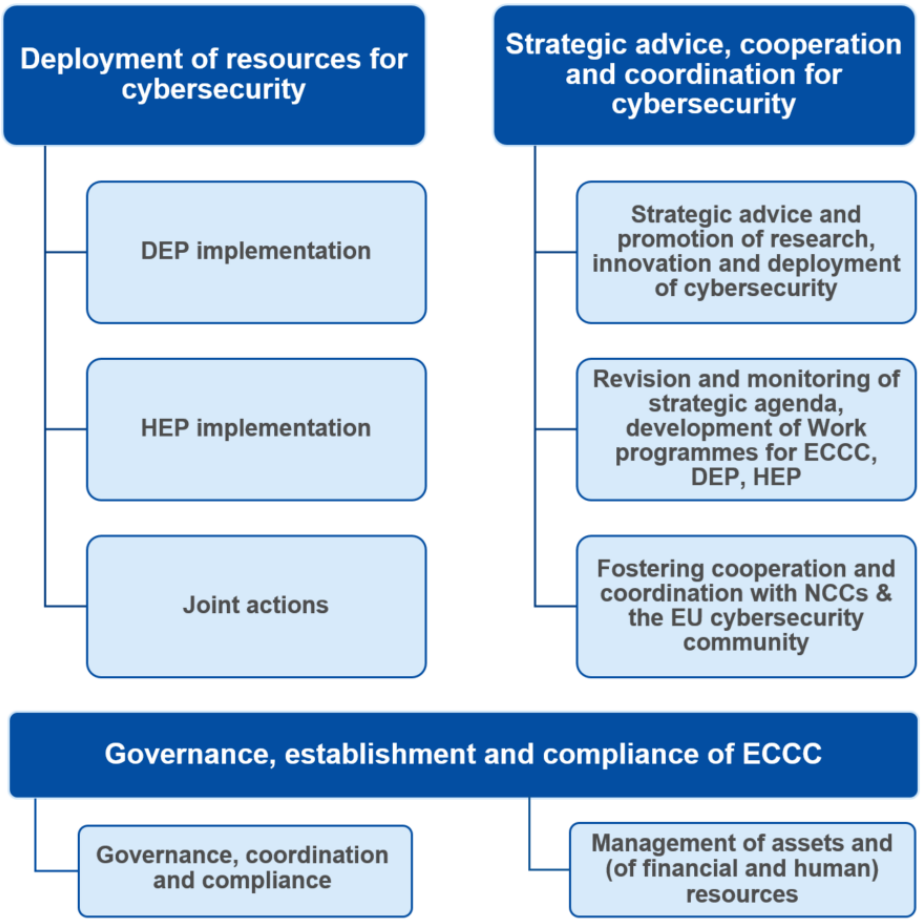
By 2025 the ECCC should be at cruising speed and tasks associated to its set-up will decrease (e.g. legal advice regarding seat agreement with host country, etc.) allowing to allocate most resources to the implementation of operational tasks.

SECTION III. WORK PROGRAMME 2025

III.1 EXECUTIVE SUMMARY

The overall objectives described in the multiannual outlook 2025-2027 are elaborated in the activities indicated in this section for the year 2025. In 2025 the focus will shift from set-up related activities to operational tasks, notably regarding DEP and HEP implementation[28], and possibly also joint actions supported with MS contributions. Other activities will include the monitoring and update of the Strategic Agenda of the ECCC, the full operation of the Network of NCCs and of the Community. Another Activity will cover all actions required to support the work of the ECCC, its operations and its staff.

The image below provides an overview of the 2025 activities. The next sections elaborate on the context, expected activities and associated results for each of the 3 activities of the SPD.



[28] DEP assumes programming and execution, HEP assumes execution while Joint actions (using both DEP and HEP funding) assume programming and execution

III.2 ACTIVITIES

III.2.1. ACTIVITY 1: Deployment of resources for cybersecurity

This Activity contributes to the objectives of Article 4 *(b) of the ECCC Regulation: "implementing actions under relevant Union funding programmes in accordance with the relevant work programmes and the Union legislative acts establishing those funding programmes;* and *(d) where relevant and appropriate, acquiring and operating ICT infrastructure and services where necessary to fulfil the tasks set out in Article 5 and in accordance with the respective work programs set out in point (b) of Article 5(3)*."

This Activity is a continuation of Activity 2 in previous SPDs of ECCC and will follow closely the Strategic Agenda adopted by ECCC GB in 2023.

Building on the work delivered in previous years, the ECCC, together with the Network of NCCs, will continue to implement the actions under Specific Objective 3 (Cybersecurity and Trust) of the DEP and specific actions under HEP. This includes the management of projects awarded under the DEP work programmes 2021-2022 and 2023-2024, as well as the publication of related calls, evaluation of proposals/tenders, signature of grants/contracts and management of the projects retained for funding under the *ECCC Work Programme implementing the cybersecurity parts of the Digital Europe Programme (in particular actions related to Article 6 of Regulation (EU) 2021/694) for 2025-2027* and HEP work programme 2025.

The Horizon Europe Work Programme for 2025 was adopted by the Commission in May 2025[29]. The Commission intends to conclude a contribution agreement with the European Cybersecurity Competence Centre (ECCC) for the implementation of Horizon Europe cybersecurity actions not co-funded by Member States, in accordance with Article 5(5) of Regulation (EU) 2021/887. Further to the contribution agreement, The ECCC will launch a call to implement the part on "Increased Cybersecurity", as specified in and in accordance with Horizon Europe Work Programme 2025 for Cluster 3[30]. For 2025, the following topics are foreseen for the call foreseen (indicatively) for June 2025 (closing in November 2025):

- HORIZON-CL3-2025-02-CS-ECCC-01: Generative AI for Cybersecurity applications
- HORIZON-CL3-2025-02-CS-ECCC-02: New advanced tools and processes for Operational Cybersecurity
- HORIZON-CL3-2025-02-CS-ECCC-03: Privacy Enhancing Technologies
- HORIZON-CL3-2025-02-CS-ECCC-04: Security evaluations of Post-Quantum Cryptography (PQC) primitives
- HORIZON-CL3-2025-02-CS-ECCC-05: Security of implementations of Post Quantum Cryptography algorithms
- HORIZON-CL3-2025-02-CS-ECCC-06: Integration of Post-Quantum Cryptography (PQC) algorithms into high-level protocols

More information on these calls is to be found in Annex XIII of the present document and in the related Work Programme as adopted.

The ECCC *Work Programme 2025-2027 implementing the cybersecurity parts of the Digital Europe Programme (in particular actions related to Article 6 of Regulation (EU) 2021/694)* was adopted by the ECCC GB, with decision no

[29] Horizon Europe Work Programme 2025, 6. Civil Security for Society, (European Commission Decision C(2025) 2779 of 14 May 2025), available at: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2025/wp-6-civil-security-for-society_horizon-2025_en.pdf

[30] Please see Horizon Europe Work Programme 2025, 6. Civil Security for Society, (European Commission Decision C(2025) 2779 of 14 May 2025), available at: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2025/wp-6-civil-security-for-society_horizon-2025_en.pdf see page 91-92 for detailed allocation of budget and type of actions.

2025/04 in March 2025[31], and subsequently amended (in June 2025 and October 2025). A high-level overview is included here below, covering the main areas of work:

- New technologies. AI & post-quantum transition
- Cyber Solidarity Implementation
- Additional actions improving EU cyber resilience
- Programme Support Actions

For the full details please consult the related *ECCC Work Programme 2025-2027 implementing the cybersecurity parts of the Digital Europe Programme,* which includes the details on the topics, their indicative planning and their budget allocation and which should be considered to complement the present document with the related information.

Its budget reflects last minute budget changes taking into account the results of the conciliation procedure with a decrease of 5 million EUR in commitment allocation for ECCC[32] and the inclusion of additional budget unused from previous year, in line with the provision in the updated ECCC Financial Regulation. The amounts unused from previous years and the reduction in budget are presented in the SPD annexes.

Important actions to be undertaken in this Activity in 2025 include the following:

Area	Expected activities	Expected results
DEP implementation	Management of projects from DEP WP 2021-2022 and WP 2023-2024. Implement DEP calls for WP 2025-2026 (take financing decisions, launch calls, organise evaluations, conclude grant agreements) taking account of the adopted Strategic Agenda Where necessary, adopt guidelines for proposals and projects, model grant agreement, methodology to calculate MS in-kind contribution	Launch call for proposals and follow up on it Fulfilment of DEP KPIs: [DEP] Indicator 3.1a: Cybersecurity infrastructure and/or tools jointly procured: 15 tools and/or infrastructures by 2027[33] [DEP] Indicator 3.1b: Cybersecurity infrastructure and/or tools deployed: 165 infrastructure (15) and/or tools (150) deployed by 2027[34] [DEP] Indicator 3.2: Users and communities getting access to European cybersecurity facilities[35] : -150 by 2027 & 300 by 2028
HEP implementation	Manage part of HEP further to EC services' delegation.	Fulfil HEP KPIs.
Joint actions	Identify possible joint actions to be supported by contributions from some MS and by EU budget from DEP or HEP	Fulfil KPIs associated with joint actions.

III.2.2 ACTIVITY 2: Strategic advice, cooperation and coordination for cybersecurity

This is a continuation of Activity 3 and 4 in previous SPDs of ECCC. The following actions are proposed:

(a) Strategic advice and promotion of research, innovation and deployment of cybersecurity

ECCC will consult its stakeholders to develop together priorities for promoting research, innovation and deployment in the area of cybersecurity. ECCC will also receive relevant input from ENISA in accordance with

[31] The *ECCC Work Programme 2025-2027 implementing the cybersecurity parts of the Digital Europe Programme* and the GB decisions on the initial version and amendments are available here: https://cybersecurity-centre.europa.eu/governing-board_en

[32] Consolidated budget amendments by budget line for 2025, 20 November 2024, available at: https://data.consilium.europa.eu/doc/document/ST-15788-2024-ADD-5-REV-1/en/pdf

[33] [Method for setting the target] The number of joint infrastructure or joint actions will be defined by the ECCC. No joint action has been defined yet.

[34] [Method for setting the target] The number of joint infrastructures or joint actions will be defined by the ECCC. It should be noted that infrastructure and tools may be of a varied nature: the target for infrastructures is 15 and the number of tools is 150.

[35] [Method for setting the target] The target is to have at least 20 Member States using each facility.

Article 5 c) of ECCC regulation[36]. The main purpose of this task is to ensure a strong European cybersecurity ecosystem that brings together the relevant stakeholders. The results from this work will contribute to the other areas of this Activity and to the dissemination efforts.

(b) Revision and monitoring of Strategic Agenda, development of ECCC Work programmes under DEP and HEP.

According to Article 2 point (8) of the Regulation, the "Agenda" is a comprehensive and sustainable cybersecurity industrial, technology and research strategy which sets out recommendations for the development and growth of the European cybersecurity industrial, technological and research sector, as well as priorities for the ECCC's activities; it is non-binding with respect to decisions to be taken on the annual work programmes. The Strategic Agenda, as adopted by the GB[37], will be regularly updated, setting out strategic recommendations for the annual work programme and the multiannual work programme. The implementation of the Strategic Agenda will be monitored.

The ECCC annual work programme will set, in accordance with the Strategic Agenda and the multiannual work programme, priorities for DEP and HEP, to what extent these will be co-financed by the MS.

EC services will take into account the input from the Strategic Agenda when preparing the HEP WP. After achieving its financial autonomy, the ECCC will prepare the cybersecurity parts of the DEP work programme and contribute to the HEP work programme in accordance with the actions set out in the Strategic Agenda.

(c) Fostering cooperation and coordination with NCCs and the EU Cybersecurity Competence Community

The Network of NCCs is composed of all NCCs notified to the GB by the MS (Article 6.7 of the Regulation). NCCs function as contact points at the national level for the Community and the ECCC (Article 7.1(a) of the Regulation). They also provide support to carry out actions under the ECCC Regulation, and they can pass on financial support to local actors (Article 7.1(f) of the Regulation). 25 MS and 3 associated countries have notified to the GB the entities acting as their NCCs.

Moreover, even dedicated Working Groups of the GB have been established, which cooperate closely with the NCCs Network (WG have been revised during 2024 and are listed below):

- *WG1: Community Building*
- *WG 2: Boost application process success*
- *WG 3: International awareness*
- *WG 4: Strategic advice*
- *WG 5: Cyber skills*
- *WG 6: Cyber Hubs*

The ECCC provides support to the NCCs Network, and to the European Cybersecurity Competence Community. A dedicated DEP Call 'Cybersecurity Community Support' (CNECT/2022/OP/0033) supports the activities of the Cybersecurity Competence Community at European level, within the scope and operations of the ECCC and the NCCs Network. The main objectives of this Action are to analyse the Cybersecurity Competence Community, link it with the ECCC and the NCCs Network, and stimulate collaboration. The Commission services monitor this Action and manages the contractor. The ECCC will undertake certain tasks in cooperation with ENISA (Article 3.2 of the Regulation) to be defined and planned in accordance to the Memorandum of Understanding (MoU) signed between the two organisations in August 2023.

The Cybersecurity Competence Community should involve a large, open, and diverse group of actors involved in cybersecurity technology, including in particular research entities, supply/demand-side industries and the

[36] The ECCC can benefit from ENISA's work in identifying research and innovation priorities as per Article 11.a) of the CSA, already resulting from extensive consultation with the EU research community and industry.
[37] Article 13.3(a) of the Regulation.

public sector that should conduct activities in line with EU strategic autonomy. It provides, particularly through the SAG, input to the activities and work plan of the ECCC, and it benefits from the Community-building activities of the ECCC and the Network.

In cooperation with the NCCs and the Community, the ECCC should increase visibility of EU cybersecurity expertise, products and services, as well as bring together resources and knowledge on cybersecurity markets and research, providing an EU-wide overview of the cybersecurity ecosystem. This is supported also through the mentioned Coordination and Support Action on the Cybersecurity Competence Community, including an "EU cybersecurity market observatory" in coordination with ENISA. The ECCC can benefit from ENISA work on surveying the market. The ECCC and ENISA can jointly coordinate the access to the network of NCCs in relation to surveys, market related data, access to databases, market analytics and research results.

Moreover, as of 2023 Iceland, Liechtenstein and Norway are full ECCC members (without vote in the GB), contributing financially to ECCC activities and benefiting from them, including support to and involvement of their NCCs and Community members.

Actions to be undertaken in the Activity 2 area during 2025 include the following:

Area	Expected activities	Expected results
Strategic advice and promotion of research, innovation and deployment of cybersecurity	Priorities for promoting research, innovation and deployment of cybersecurity Dissemination activities and strategic advice	Develop or update priorities for promoting research, innovation and deployment of cybersecurity Dissemination activities and strategic advice ECCC supports the respective Working Groups of the ECCC GB and its Chairs as secretariat and is seeking collaboration with ENISA.
Revision and monitoring of Strategic Agenda, development of Work programmes for ECCC, DEP, HEP	**Strategic Agenda** Revision of the adopted Strategic Agenda, following consultation with all relevant actors (EC, NCCs, Community, ENISA, SAG) to prepare next version of the Strategic Agenda Monitoring the implementation of the previous Strategic Agenda adopted in 2023. Periodic reporting on the monitoring of the Strategic Agenda. Dissemination of the Agenda to relevant stakeholders, including the HEP Program Committee **Work programmes related activities** Development, adoption and monitoring of the multiannual work programme and the annual work programme for ECCC and for DEP and HEP	- Preparation of the revised version of the Strategic Agenda by Q3/25 - Report on the implementation of the current Strategic Agenda by Q2/25 - Contributions to dissemination activities regarding the Agenda and research and innovation priorities - Delivery of draft and final SPDs by statutory deadlines - Report on the implementation of the 2025-2027 DEP Work Programme by Q4/25 - Timely input into the consultation related to DEP or HEP
Fostering cooperation and coordination with NCCs and the EU cybersecurity competence community	**Network of National Coordination Centres:** Complete the setting-up of the Network and smooth functioning as an integrated Network Implement and update the indicative "service catalogue" for NCCs Further definition and implementation of modalities of interaction between the ECCC and the Network of NCCs (coordination mechanisms, alignment of activities, organisation of workshops/recurrent meetings, etc.) **Cybersecurity Competence Community (stakeholders):** Community registrations and development of associated tools Support new Community registrations, develop relevant tools and stimulate activities Community participation to the activities of the working groups, where relevant Maintain the EU "cybersecurity market observatory" in coordination with ENISA	- The Network of National Coordination Centres (NCCs) is fully established and functioning seamlessly, enabling effective communication and collaboration among member countries with approved rules of procedures and reporting forms by Q2/25 - A comprehensive and up-to-date "service catalogue" for NCCs is implemented and maintained. This catalogue outlines the range of common services and capabilities offered by NCCs to the Cybersecurity Competence Community (CCC) by Q4/25 ECCC facilitates the registration process of national members to the CCC, including on clear organisational and technical guidelines. - Well-defined and efficient coordination mechanisms are established between the ECCC and the Network of NCC set up by Q3/25. Regular workshops and meetings are organized to facilitate alignment of activities, sharing of best practices, and collaborative efforts. - Measures to sustain the NCC's to ensure the continuous functioning of the network and ensuring appropriate funding in line with DEP WP.

III.2.3 ACTIVITY 3: Governance, establishment and compliance of ECCC

This Activity is a continuation of the Activity 1 in previous SPDs, dedicated to set up the operational activities of the ECCC during its growing stage.

The Activity focusses on all the managerial and administrative activities required to support the operational tasks of the ECCC. As already stated in previous SPDs, after achieving its financial autonomy, the ECCC will focus mainly on its operational tasks, benefitting from the governance structures, rules, procedures and infrastructure in place. As of 2025, the focus will be on ensuring efficient and effective use of existing resources.

The main actions are as follows:

- Governance, coordination and compliance
  - ED office, coordination and management of the ECCC.
  - Planning and programming activities and documents.
  - Relation with GB and ECCC stakeholders including host country; Secretariat for ECCC GB.
  - Liaison activities with other EU bodies in the remit of ECCC mandate.
  - Compliance and internal control.
  - Communication, dissemination and outreach.
- Management of assets and (of financial and human) resources
  - Efficient and effective management of financial and human resources.
  - Consolidate IT tools, ICT assets, security rules and other logistical aspects.
  - Building and facilities management, including environmental management.
  - Relations with host country and adequate implementation of the Host Agreement.
  - Monitoring, evaluations, access to documents, reporting.

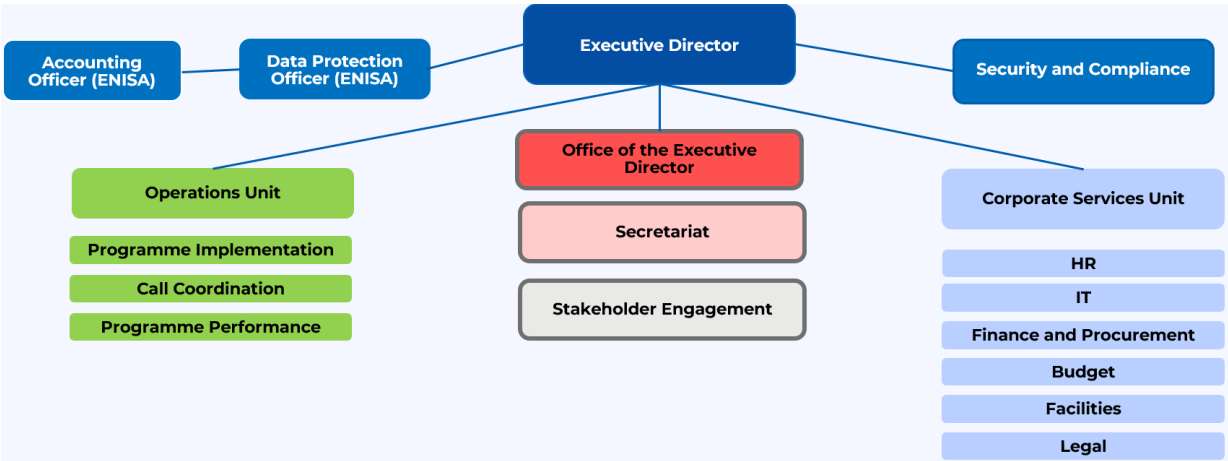
Actions to be undertaken in this Activity area in 2025 include the following:

Area	Expected activities	Expected results
Governance, coordination and compliance	ED office, coordination and management of ECCC Planning and related programming activities and documents. Implement performance indicators. Relation with GB and ECCC stakeholders including host MS; Secretariat for ECCC GB Liaison activities with the other EU bodies in the remit of ECCC mandate Compliance and internal control Communication, dissemination and outreach	- Timely preparation, consultations, reviews and adoption of documents dedicated to planning and programming in line with the agreed timelines. - Transparency in decision making and involvement of relevant staff or staff committee as appropriate. - Satisfactory support to the relevant stakeholders – to be measure with a survey in Q3/25 - SLAs and MoUs agreed indicating the associated efficiency gains - High level of compliance with reduced number of recommendations following audits - Communication strategy development and implementation by Q4/25
Management of assets and (of financial and human) resources	Consolidate financial and human resources Consolidate IT tools, ICT assets, security rules and other logistics aspects Building and facilities management, including environmental management Relations with host MS and adequate implementation of the Host Agreement Monitoring, evaluations, access to documents, reporting	- Budget implementation in line with the ICF KPI - HR policies and implementing rules in place, satisfaction of staff (survey launched in Q1/25) - Sustainable and environmentally friendly working conditions (survey launched in Q2/25) - Coordination team with Host Country set up by Q1/25 - Timely reporting and timely follow up on requests, evaluations and recommendations

ANNEXES

ANNEX I. ORGANISATION CHART

The organisation chart as adopted by the ED of ECCC in March 2025 is presented here below.



ANNEX II. RESOURCE ALLOCATION PER ACTIVITY 2025 – 2027

Resource allocation forecast is introduced below, with aggregated values.

No	Activity name	2025			2026			2027		
		TA	CA & SNE (FTEs)	Budget (EUR)	TA	CA & SNE (FTEs)	Budget (EUR)	TA	CA & SNE (FTEs)	Budget (EUR)
1	Deployment of resources for cybersecurity	4	15	237,061,046.86	4	15	124,151,074.60	4	15	118,675,096.65
2	Strategic advice, cooperation and coordination for cybersecurity	3	3	412,984.69	3	3	444,925.89	3	3	471,335.33
3	Governance, establishment and compliance of the ECCC	3	10	1,394,550.00	3	10	1,503,400.00	3	10	1,245,765.51
Total		10	28	238,868,581.55	10	28	126,099,400.49	10	28	120,392,197.49

ANNEX III. FINANCIAL RESOURCES 2025 - 2027

Budget Revenue[38]

In accordance with the provisions of the legal framework applicable to the ECCC, for 2025 the only contributor is the EU with the budget planned for Cybersecurity activities in the DEP and in Horizon Europe Programme[39]. These contributions will cover both the administrative and operational costs of the ECCC. Contributions from the MS may be taken up with an amendment of the WP and the budget. The ECCC global budget revenues for the period 2025-2027 are presented in:

- Table 1a – Overview table for Revenue of commitment appropriations.
- Table 2a – Overview table for Revenue of payment appropriations.

[38] 2024 figures in the tables are based on the Initial budget for 2024. 2025 figures are based on the total financial envelope for ECCC as envisaged in the 2025 draft EU budget.
EFTA percentages for DEP - 2,93 % in 2023; 3.58% for 2024 and 2.79% in 2025-2027.
[39] This amended version includes the amount of EUR 90 550 000 stemming from a Contribution agreement with the EC.

In the current budget (2025) the ECCC, is also reactivating credits coming from previous years and that can be carry forward in line with the provision in the ECCC Financial Regulation[40]. For 2025, the amount to be transferred is of EUR 42 622 717.73 of commitment appropriations. These credits will be partly used for covering the expenditure for DEP in line with the priorities raised by the ECCC Governing Board.

The global revenue includes (within the indicated financial envelope) the amounts stemming from the implementation of tasks under Horizon Europe through the signature of a Contribution Agreement for Revenue in terms of commitment and payment appropriations respectively.

The current amendment 2 reduces the revenue (commitment appropriations) of ECCC by EUR 15 000 000 due to the amendment of the DEP Cybersecurity Work Programme for 2025.

The previous amendment 1 introduced:

A. Revenue (commitment appropriations) for EUR 90 550 000 stemming from through the signature of a Contribution Agreement for the implementation of Horizon Europe cybersecurity actions, not co-funded by Member States, in accordance with Article 5(5) of Regulation (EU) 2021/8878.

B. Revenue (payment appropriations) for EUR 55 000 000 necessary to honour the respective legal and budgetary commitments (related to the HEP) from previous financial years.

Table 1a – Overview table – General revenue, commitment appropriations

Revenue	2024	2025	2025	2025	2025
	Final budget	Initial budget	Amendment 1	Amendment 2	Final budget
ontribution	211,267,742.00	160,042,567.73	0.00	-14,592,859.23	145,449,708.50
d countries contribution	7,563,385.16	3,276,013.82	0.00	-407,140.77	2,868,873.05
er Contributions	96,495,097.06	p.m.	90,550,000.00	0.00	90,550,000.00
AL REVENUES	315,326,224.22	163,318,581.55	90,550,000.00	-15,000,000.00	238,868,581.55

Table 1b – Detailed table – Revenues, commitment appropriations

REVENUES	General revenues, commitment appropriations										
	Budget 2023	Budget 2024	2025						VAR 2025/2024 (%)	Envisaged 2026	Envisaged 2027
			Agency request	Re-activated credits from previous years **	2025 budget	Amendment 1	Amendment 2	Final 2025 budget			
1 REVENUE FROM FEES AND CHARGES											
2 EU CONTRIBUTION	179,058,443.00	211,267,742.00	117,419,850.00	42,622,717.73	160,042,567.73	0.00	-14,592,859.23	145,449,708.50	-31%	122,676,720.00	117,124,426.00
- Of which assigned revenues deriving from previous years' surpluses											
3 THIRD COUNTRIES CONTRIBUTION (incl. EEA/EFTA and candidate countries)	5,246,412.00	7,563,385.16	3,276,013.82	0.00	3,276,013.82	0.00	-407,140.77	2,868,873.05	-62%	3,422,680.49	3,267,771.49
- Of which EEA/EFTA (excl. Switzerland)	*5,246,412.00*	*7,563,385.16*	*3,276,013.82*	*0.00*	*3,276,013.82*	*0.00*	*-407,140.77*	*2,868,873.05*	-62%	*3,422,680.49*	*3,267,771.49*
- Of which candidate countries											
4 OTHER CONTRIBUTIONS		96,495,097.06	p.m.	p.m.	p.m.	90,550,000.00	0.00	90,550,000.00	-6%		
5 ADMINISTRATIVE OPERATIONS											
- Of which interest generated by funds paid by the Commission by way of the EU contribution (FFR Art. 58)											
6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT											
7 CORRECTION OF BUDGETARY IMBALANCES											
TOTAL	184,304,855.00	315,326,224.22	120,695,863.82	42,622,717.73	163,318,581.55	90,550,000.00	-15,000,000.00	238,868,581.55	-24%	126,099,400.49	120,392,197.49

(*) This is based on the the following EFTA percentage for DEP: 2,93 % in 2023; 3.58% for 2024 and 2.79% in 2025-2027.

(**) This follows a GB decision from March 2024 for re-activation of credits in line with the N+3 rule (Art. 12 of the ECCC Financial Rules).

Table 2a – Overview table - Total Revenue, payment appropriations

Revenue	2024	2025	2025	2025	2025
	Final budget	Initial budget	Amendment 1	Amendment 2	Final budget
EU contribution	153,362,452.21	186,753,417.00	0.00	0.00	186,753,417.00
Third countries contribution	5,490,375.79	5,210,420.33	0.00	0.00	5,210,420.33
Other Contributions	16,903,783.89	p.m.	55,000,000.00	0.00	55,000,000.00
TOTAL REVENUES	175,756,611.89	191,963,837.33	55,000,000.00	0.00	246,963,837.33

[40] Art 12 of the ECCC Financial Rules

Table 2b – Detailed table - Total Revenue, payment appropriations

REVENUES	General revenues, payment appropriations										
	Budget 2023	Budget 2024	2025						VAR 2025/2024 (%)	Envisaged 2026	Envisaged 2027
			Agency request	Re-activated credits from previous years **	2025 budget	Amendment 1	Amendment 2	Final 2025 budget			
1 REVENUE FROM FEES AND CHARGES											
2 EU CONTRIBUTION	179,058,443.00	153,362,452.21	186,753,417.00	0.00	186,753,417.00	0.00	0.00	186,753,417.00	22%	122,676,720.00	117,124,426.00
- Of which assigned revenues deriving from previous years' surpluses											
3 THIRD COUNTRIES CONTRIBUTION (incl. EEA/EFTA and candidate countries)	5,246,412.00	5,490,375.79	5,210,420.33	0.00	5,210,420.33	0.00	0.00	5,210,420.33	-5%	3,422,680.49	3,267,771.49
- Of which EEA/EFTA (excl. Switzerland)	*5,246,412.00*	*5,490,375.79*	*5,210,420.33*		*5,210,420.33*	*0.00*	*0.00*	*5,210,420.33*	-5%	*3,422,680.49*	*3,267,771.49*
- Of which candidate countries											
4 OTHER CONTRIBUTIONS		16,903,783.89	p.m.	p.m.	p.m.	55,000,000.00	0.00	55,000,000.00	225%		
5 ADMINISTRATIVE OPERATIONS											
- Of which interest generated by funds paid by the Commission by way of the EU contribution (FFR Art. 58)											
6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT											
7 CORRECTION OF BUDGETARY IMBALANCES											
TOTAL	184,304,855.00	175,756,611.89	191,963,837.33	0.00	191,963,837.33	55,000,000.00	0.00	246,963,837.33	41%	126,099,400.49	120,392,197.49

(*) This is based on the the following EFTA percentage for DEP: 2,93 % in 2023; 3.58% for 2024 and 2.79% in 2025-2027.
(**) This follows a GB decision from March 2024 for re-activation of credits in line with the N+3 rule (Art. 12 of the ECCC Financial Rules).

Budget Expenditure

The ECCC total budget expenditure for the period 2025-2027, including Amendment 1 and Amendment 2, are presented in table 5a and the detailed allocation of expenditure is revealed in:

- Table 5b – Detailed expenditure, commitment appropriations.
- Table 5c – Detailed expenditure, payment appropriations.

In this SPD, the ECCC introduced also minor changes to the budgetary structure in alignment with the common practices from other EU Agencies and bodies.

The current amendment 2 reduces the revenue (commitment appropriations) of ECCC by EUR 15 000 000 due to the amendment of the DEP Cybersecurity Work Programme for 2025.

The previous amendment 1 introduced:

A. Revenue (commitment appropriations) for EUR 90 550 000 stemming from through the signature of a Contribution Agreement for the implementation of Horizon Europe cybersecurity actions, not co-funded by Member States, in accordance with Article 5(5) of Regulation (EU) 2021/8878.

B. Revenue (payment appropriations) for EUR 55 000 000 necessary to honour the respective legal and budgetary commitments (related to the HEP) from previous financial years.

The EU budget will constitute a ceiling for the actual EU contribution, in accordance with Article 21 of the Regulation. The amount of MS contributions, if any, will be determined by the MS themselves.

Table 5a – Overview - Expenditure, commitment and payment appropriations

Expediture	2024		2025 (incl. Amendments 1 and 2)	
	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations
Title 1 - Staff expenditure	1,747,000	1,747,000	3,528,500	3,528,500
Title 2 - Infrastructure and operating expenditure	901,000	901,000	960,000	960,000
Title 3 - Operational expenditure	312,678,224	173,108,612	234,380,082	242,475,337
TOTAL Expenditure	315,326,224	175,756,612	238,868,582	246,963,837

Commitment appropriations

Table 5b – Detailed Expenditure, commitment appropriations

Budget line	EXPENDITURE	Commitment appropriations										
		Budget 2023	Budget 2024	2025 Agency request	2025 Re-activated credits from previous years **	2025 2025 budget	2025 Amendment 1	2,025.00 Amendment 2	2025 Final 2025 budget	VAR 2025/2024 (%)	Envisaged 2026	Envisaged 2027
Title 1	**Title 1 - Staff expenditure**	**1,560,000.00**	**1,747,000.00**	**3,528,500.00**	**0.00**	**3,528,500.00**	**0.00**	**0.00**	**3,528,500.00**	**102%**	**3,815,500.00**	**4,073,640.00**
1111	Salaries and allowances for temporary and permanent staff	882,000.00	950,000.00	1,350,000.00		1,350,000.00			1,350,000.00	42%	1,458,000.00	1,560,060.00
1121	Salaries and allowances for contractual agents	440,000.00	500,000.00	1,800,000.00		1,800,000.00			1,800,000.00	260%	1,944,000.00	2,080,080.00
1131	Seconded national experts, interim staff and trainees	62,000.00	100,000.00	100,000.00		100,000.00			100,000.00	0%	120,000.00	130,000.00
1141	Trainings and Recruitment	124,000.00	155,000.00	183,500.00		183,500.00			183,500.00	18%	183,500.00	183,500.00
1151	Social welfare and medical services	52,000.00	42,000.00	95,000.00		95,000.00			95,000.00	126%	110,000.00	120,000.00
Title 2	**Title 2 - Infrastructure and operating expenditure**	**833,239.00**	**901,000.00**	**960,000.00**	**0.00**	**960,000.00**	**0.00**	**0.00**	**960,000.00**	**7%**	**1,025,000.00**	**1,045,000.00**
2111	Rental of building and associated costs	156,000.00	290,000.00	60,000.00		60,000.00			60,000.00	-79%	70,000.00	80,000.00
2121	Computer centre operations and data processing	62,000.00	290,000.00	350,000.00		350,000.00			350,000.00	21%	380,000.00	380,000.00
2131	Moveable property and associated costs	353,912.00	218,000.00	100,000.00		100,000.00			100,000.00	-54%	100,000.00	100,000.00
2141	Current administrative expenditure	261,327.00	103,000.00	450,000.00		450,000.00			450,000.00	337%	475,000.00	485,000.00
Title 3	**Title 3 - Operational expenditure**	**181,911,616.00**	**312,678,224.22**	**116,207,363.82**	**42,622,717.73**	**158,830,081.55**	**90,550,000.00**	**-15,000,000.00**	**234,380,081.55**	**-25%**	**121,258,900.49**	**115,273,557.49**
3111	DEP Programme	181,385,616.00	215,731,127.16	114,717,363.82	42,622,717.73	157,340,081.55		-15,000,000.00	142,340,081.55	-34%	119,738,900.49	113,743,557.49
3121	Horizon Programme		96,495,097.06	0.00		p.m.	90,550,000.00		90,550,000.00	-6%	0.00	0.00
3131	Evaluations and Programme tools			1,000,000.00		1,000,000.00			1,000,000.00	-	1,000,000.00	1,000,000.00
3141	Publication, communication and trasnlation costs	100,000.00	150,000.00	110,000.00		110,000.00			110,000.00	-27%	130,000.00	130,000.00
3151	Statutory, technical meetings and Studies	218,000.00	222,000.00	200,000.00		200,000.00			200,000.00	-10%	200,000.00	200,000.00
3161	Missions	208,000.00	80,000.00	180,000.00		180,000.00			180,000.00	125%	190,000.00	200,000.00
	TOTAL	**184,304,855.00**	**315,326,224.22**	***120,695,863.82***	***42,622,717.73***	**163,318,581.55**	**90,550,000.00**	**-15,000,000.00**	**238,868,581.55**	**-24%**	**126,099,400.49**	**120,392,197.49**

*** Remark: This follows a GB decision from March 2024 for re-activation of credits in line with the N+3 rule (Art. 12 of the ECCC Financial Rules).*

Payment appropriations

Table 5c – Detailed Expenditure, payment appropriations

Budget line	EXPENDITURE	Payment appropriations										
		Budget 2023	Budget 2024	2025 Agency request	2025 Re-activated credits from previous years **	2025 2025 budget	2025 Amendment 1	2,025.00 Amendment 2	2025 Final 2025 budget	VAR 2025/2024 (%)	Envisaged 2026	Envisaged 2027
Title 1	**Title 1 - Staff expenditure**	**1,560,000.00**	**1,747,000.00**	**3,528,500.00**	**0.00**	**3,528,500.00**	**0.00**		**3,528,500.00**	**102%**	**3,815,500.00**	**4,073,640.00**
1111	Salaries and allowances for temporary and permanent staff	882,000.00	950,000.00	1,350,000.00		1,350,000.00			1,350,000.00	42%	1,458,000.00	1,560,060.00
1121	Salaries and allowances for contractual agents	*440,000.00*	*500,000.00*	*1,800,000.00*		1,800,000.00			1,800,000.00	260%	*1,944,000.00*	*2,080,080.00*
1131	Seconded national experts, interim staff and trainees	*62,000.00*	*100,000.00*	*100,000.00*		100,000.00			100,000.00	0%	*120,000.00*	*130,000.00*
1141	Trainings and Recruitment	124,000.00	155,000.00	183,500.00		183,500.00			183,500.00	18%	183,500.00	183,500.00
1151	Social welfare and medical services	52,000.00	42,000.00	95,000.00		95,000.00			95,000.00	126%	110,000.00	120,000.00
Title 2	**Title 2 - Infrastructure and operating expenditure**	**833,239.00**	**901,000.00**	**960,000.00**	**0.00**	**960,000.00**	**0.00**		**960,000.00**	**7%**	**1,025,000.00**	**1,045,000.00**
2111	Rental of building and associated costs	156,000.00	290,000.00	60,000.00		60,000.00			60,000.00	-79%	70,000.00	80,000.00
2121	Computer centre operations and data processing	62,000.00	290,000.00	350,000.00		350,000.00			350,000.00	21%	380,000.00	380,000.00
2131	Moveable property and associated costs	353,912.00	218,000.00	100,000.00		100,000.00			100,000.00	-54%	100,000.00	100,000.00
2141	Current administrative expenditure	261,327.00	103,000.00	450,000.00		450,000.00			450,000.00	337%	475,000.00	485,000.00
Title 3	**Title 3 - Operational expenditure**	**224,438,363.00**	**173,108,611.89**	**187,475,337.34**	**0.00**	**187,475,337.34**	**55,000,000.00**		**242,475,337.34**	**40%**	**121,258,900.49**	**115,273,557.49**
3111	DEP Programme	223,912,363.00	155,752,828.00	185,985,337.34	0.00	185,985,337.34			185,985,337.34	19%	119,738,900.49	113,743,557.49
3121	Horizon Programme		16,903,783.89	0.00		p.m.	55,000,000.00		55,000,000.00	225%	0.00	0.00
3131	Evaluations and Programme tools			1,000,000.00		1,000,000.00			1,000,000.00	-	1,000,000.00	1,000,000.00
3141	Publication, communication and trasnlation costs	100,000.00	150,000.00	110,000.00		110,000.00			110,000.00	-27%	130,000.00	130,000.00
3151	Statutory, technical meetings and Studies	218,000.00	222,000.00	200,000.00		200,000.00			200,000.00	-10%	200,000.00	200,000.00
3161	Missions	208,000.00	80,000.00	180,000.00		180,000.00			180,000.00	125%	190,000.00	200,000.00
	TOTAL	**226,831,602.00**	**175,756,611.89**	**191,963,837.34**	**0.00**	**191,963,837.34**	**55,000,000.00**	**0.00**	**246,963,837.34**	**41%**	**126,099,400.49**	**120,392,197.49**

*** Remark: This follows a GB decision from March 2024 for re-activation of credits in line with the N+3 rule (Art. 12 of the ECCC Financial Rules).*

Details on the use of financial resources

The description below follows the new budgetary structure which is proposed to enter into force as from financial year 2025.

The key changes encompass the following:

- Appropriations for mission are reallocated from Title 1 to Title 3.
- Certain budget lines are merged – for instance recruitment and training costs.
- Some budget lines with low appropriations on them are absorbed into other budget lines (the budget line for Insurance against sickness, accidents, occupational disease, unemployment and related is integrated into Salaries and allowances for temporary agents).

- The Publication, communication and translation costs, together with the External activities / studies, technical and statutory meetings are reallocated from Title 2 to Title 3.

The appropriations from the previous years (2023 and 2024) are presented in accordance with the new budgetary structure to ensure comparability and transparency.

We present below the list of budgetary items included in each title according to the newly proposed budget nomenclature.

TITLE 1

This appropriations from this title will cover the staff-related expenditure of the Centre, amongst which:

- the remuneration (salaries and allowances) of the temporary and contractual staff in accordance with the Staff Regulations.
- Training and recruitment costs.
- insurances and medical check-up of staff and associated analyses required.
- other staff-related expenses.

Details are revealed in the relevant budgetary tables.

TITLE 2

The appropriations from this title (Infrastructure and Operating expenditure) will cover the following main items:

- Logistical costs – utility costs, furniture and equipment of Permanent office, office supplies etc.
- IT infrastructure, equipment and data processing
- Current administrative expenditure etc.

TITLE 3

The title accommodates the appropriations for the operational expenditure of the ECCC, taking of board the differentiated character of the budgetary credits in the title, i.e. the distinction between commitment and payment appropriations and their separate management.

The expenditure items, under the newly introduced budgetary structure, include appropriations for:

- Digital Europe Programme.
- Horizon Europe programme.
- Evaluation and Programme tools.
- Publication, communication and translation costs.
- Statutory, technical meetings and studies.
- Missions.

ANNEX IV. HUMAN RESOURCES QUANTITATIVE

Table 1 - Staff population and its evolution; Overview of all categories of staff

A. Statutory staff and SNE (Status 31 December 2024)

STAFF	2023			2024			2025	2026	2027
ESTABILISHMENT PLAN POSTS	Authorised Budget	Filled in as of 31/12	Occupancy rate %	Authorised Budget	Filled in as of 31/12	Occupancy rate %	Authorised Budget	Authorised Budget	Authorised Budget
Administrators (AD)	10	5	50	10	6	60	10	10	10
Assistants (AST)									
TOTAL ESTABILISHMENT PLAN POSTS	10	5	50	10	6	60	10	10	10
EXTERNAL STAFF	FTE corresponding to authorised budget	Executed as of 31/12	Execution rate %	FTE corresponding to authorised budget	Executed as of 31/12	Execution rate %	FTE corresponding to authorised budget	FTE corresponding to authorised budget	FTE corresponding to authorised budget
Contract Agents (CA)	27	24	89	27	21	78	27	27	27
Seconded National Experts (SNE)	1	0		1			1	1	1
TOTAL EXTERNAL STAFF	28	24	86	28	21	75	28	28	28
TOTAL STAFF	38	29	76	38	27	71	38	38	38

B. Additional external staff expected to be financed from grant, contribution or service-level agreements

Not applicable.

C. C. Other Human Resources

Structural service providers[41]

	Actually in place as of 31/12/2023
Security	0
IT	0
Other (specify)	0
.....	

Interim workers

	Total FTEs in year 2023
Number	1

Table 2 – Multi-annual staff policy plan 2025, 2026, 2027

Function group and grade	2023				2024		2025		2026		2027	
	Authorised Budget		Actually filled as of 31/12/2023		Authorised Budget		Envisaged		Envisaged		Envisaged	
	Permanent posts	Temporary posts	Permanent posts	Temporary posts	Permanent posts	Temporary posts	Permanent posts	Temporary posts	Permanent posts	Temporary posts	Permanent posts	Temporary posts
AD 16												
AD 15												
AD 14		1		0		1		1		1		1
AD 13												1
AD 12		2		0		2		2		2		2
AD 11		2		0		2		2		2		1
AD 10												
AD 9										1		2
AD 8		3		3		3		3		3		3
AD 7		2		2		2		2		1		
AD 6												
AD 5												
AD TOTAL		10		5		10		10		10		10
AST 11												
AST 10												
AST 9												
AST 8												
AST 7												
AST 6												
AST 5												
AST 4												
AST 3												
AST 2												
AST 1												
AST TOTAL		0		0		0		0		0		0
AST/SC 6												
AST/SC 5												
AST/SC 4												
AST/SC 3												
AST/SC 2												
AST/SC 1												
AST/SC TOTAL		0		0		0		0		0		0
TOTAL		10		5		10		10		10		10
GRAND TOTAL		10		5		10		10		10		10

[41] (6) Service providers are contracted by a private company and carry out specialized outsourced tasks of a horizontal/support nature. At the Commission, following general criteria should be fulfilled: 1) no individual contract with the Commission 2) on the Commission premises, usually with a PC and desk 3) administratively followed by the Commission (badge, etc.) and 4) contributing to the added value of the Commission

- External personnel

Contract Agents*

Contract agents	Authorised 2024	Recruited as of 31/12/2024	2025 estimate	Draft Budget 2026 estimate
Function Group IV	21	16	21	21
Function Group III	2	2	2	2
Function Group II	4	3	4	4
Function Group I	0	0	0	0
Contract Agents	21	21	27	27

**For Contract Agents, for the years 2025-2027, while the total number is the same, the function groups were revised and updated upwards to take into account the change in the job profiles and tasks that are performed after autonomy.*

Seconded National Experts

Seconded National Experts	FTE corresponding to the authorised budget 2023	Executed FTE as of 31/12/2023	Headcount as of 31/12/2023	FTE corresponding to the authorised budget 2024	FTE corresponding to the authorised budget 2025	FTE corresponding to the authorised budget 2026	FTE corresponding to the authorised budget 2027
TOTAL	1	0	0	1	1	1	1

Table 3, recruitment forecasts 2024 following retirement/mobility or new requested posts is not applicable due to early state of ECCC set-up. To be updated in future SPDs, if applicable.

Number of inter-agency mobility year 2023 from and to the ECCC: 0.

ANNEX V. HUMAN RESOURCES QUALITATIVE

Statistics on past years will be provided starting from next SPD as the data available at the moment is too limited for being meaningful.

A. Recruitment policy

All implementing rules required for recruitment are in place. Further HR related rules might be adopted by the GB.

		Yes	No	If no, which other implementing rules are in place
Engagement of CA	Model Decision C(2019)3016	X		
Engagement of TA	Model Decision C(2015)1508	X		
Middle management	Model decision C(2018)2540	X		
Type of posts	Model Decision C(2018)8800	X		

B. Appraisal and reclassification/promotions

		Yes	No	If no, which other implementing rules are in place
Reclassification of TA	Model Decision C(2015)9560	X		
Reclassification of CA	Model Decision C(2015)9561	X		

C. Gender representation

The ECCC has reached an overall gender balance with female staff representing 59 % of the workforce including most of the Program Officers. The distribution is not equal between temporary staff and contract agents, and this will be taken into account -if possible- in line with the Gender Equality Strategy 2020-2025[42]. However, it should be noted that, due to limited number of CA positions available at the moment the possibility to skew significantly the current distribution is very limited.

Table – **Data for 31/12/2023 - statutory staff**

		Official		Temporary		Contract Agents		Grand Total	
		staff	%	Staff	%	Staff	%	Staff	%
Female	Administrator level			1	20%	15	68%	16	59%
	Assistant level (AST & AST/SC)			0	0%	0	0%	0	0%
	Total			1	20%	15	68%	16	59%
Male	Administrator level			4	80%	7	32%	11	41%
	Assistant level (AST & AST/SC)			0	0%	0	0%	0	0%
	Total			4	80%	7	32%	11	41%
Grand Total				**5**	**100%**	**22**	**100%**	**27**	**100%**

D. Geographical Balance

Table – Data for 31/12/2023 - statutory staff only

Nationality	AD +CA FG IV		AST/SC - AST + CA FGI / CA FGII / CA FGIII		Total	
	Number	% of total staff member in AD and FGIV categories	Number	% of total staff members in AST SC/AST and FG I, II and III categories	Number	% of total staff
Romanian	14	61%	4	100%	18	67%
Italian	4	17%	0	0%	4	15%
Greek	1	4%	0	0%	1	4%
Cypriot	1	4%	0	0%	1	4%
German	1	4%	0	0%	1	4%
Polish	1	4%	0	0%	1	4%
Bulgarian	1	4%	0	0%	1	4%
Total	**23**	**100%**	**4**	**100%**	**27**	**100%**

While the ECCC should seek as much as possible geographical diversity in its coming recruitments, it should be noted that most applications received so far are from Romanian nationals.

E. Schooling

In June 2024 the ECCC GB adopted the Decision no GB/2024/5 on a schooling policy for the education costs for children of the ECCC staff members. The GB/2024/5 Decision was complemented in September 2024 by Decision of ECCC ED, No ED/2024/9, which establishes an economic ceiling to the schooling policy of the ECCC: a maximum of €17,000 per year per child enrolled in middle or high school (secondary education), and a maximum of €11,000 per year per child enrolled in primary school (elementary education).

[42] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "A Union of Equality: Gender Equality Strategy 2020-2025", COM/2020/152 final. Available here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0152.

ANNEX VI. ENVIRONMENT MANAGEMENT

Not applicable until permanent premises of ECCC are operational – handover scheduled for in Q1/2025.

ANNEX VII. BUILDING POLICY

The ECCC headquarters is located in Bucharest. The ECCC opened its Temporary Premises in Bucharest located at the Politehnica Campus building in 2023. The ECCC also concluded an Administrative Agreement with the EC Representation in Bucharest, enabling ECCC staff to use the premises of EC Representation within the scope of the Administrative Agreement. The ECCC is now scheduled to move to its Permanent Premises in Q1/25. The process may follow the specific provisions regarding building projects as indicated in Article 266 of the Financial Regulation applicable to the general budget of the EU.

ANNEX VIII. PRIVILEGES AND IMMUNITIES

The hosting agreement has been signed on 27 September 2024 and needs to be ratified to inter into force. The conclusion of the Host Agreement between the Government of Romania and the European Cybersecurity Industrial, Technology and Research Competence Centre means that the Competence Centre's premises, excluding parking places, are inviolable and exempt from search, requisition, or seizure, and its property, assets, and funds are immune from legal proceedings without the approval of the Court of Justice of the European Union. The Centre's archives, official correspondence, and documents are also inviolable.

The Executive Director, staff, and their family members (within the definition given by the Host Agreement) will receive a special residence card from Romania's Ministry of Foreign Affairs, granting them diplomatic privileges and immunities. Non-Romanian nationals, including the Executive Director and their household, are accorded the same privileges as heads of diplomatic missions under the Vienna Convention, with additional benefits like car plates and residential protection upon request. If Romania grants more favourable privileges to other EU bodies in the future, the Centre and its staff will automatically receive the same treatment. Representatives of Member States participating in the Centre's work also enjoy customary privileges and immunities during their duties. Despite these privileges, the Centre, its Executive Director, and staff must respect Romanian laws and cooperate with authorities for the proper administration of justice.

ANNEX IX. EVALUATIONS

To be updated in next versions.

ANNEX X. STRATEGY FOR THE ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL SYSTEMS

After the adoption of the Financial Regulation and the rules for the prevention, identification and resolution of conflict of interest (in respect of its members, bodies and staff, including the ED and the GB members, and the SARG members) by the Governing Board, the ECCC has adopted its Internal Control Framework in December 202343. In line with the Internal Control Framework developed by European Commission, it consists of five internal control components and 17 principles based on the COSO 2013 Internal Control-Integrated Framework.

The ECCC relies on the ENISA accounting officer (based on the Service Level Agreement signed between the ECCC and ENISA) who certifies the year-end accounts, providing reasonable assurance that the accounts present a true and fair view of the financial situation.

[43] DECISION No GB/2023/12 of the Governing Board of the European Cybersecurity Competence Centre on the Internal Control Framework for effective management applicable to the European Cybersecurity Competence Centre

The ECCC's Anti-Fraud Strategy, which is developed in line with OLAF's Methodology and guidance for the anti-fraud strategies of EU decentralised agencies and Joint Undertakings, has been adopted by the GB in June 2024[44], following a standalone fraud risk assessment exercise. It includes as annex the Action Plan for its implementation, which contains concrete actions for addressing the identified fraud risks.

ANNEX XI. PLAN FOR GRANT, CONTRIBUTION OR SERVICE-LEVEL AGREEMENTS

The ECCC does not receive any form of grant.

A Contribution Agreement, related to Digital Europe and Horizon Europe Programme, was signed for 2024 and is expected that a new one will be signed in 2025.

The ECCC initiated in 2021 the process of concluding a number of SLAs and agreements that the ECCC has to undertake during the establishment phase in order to launch recruitments and reach operational autonomy. The preparatory work started in 2021 and has resulted to concrete agreements in the course of 2022, while further work took place in 2023 and 2024 to support the transition to the financial autonomy. The table below presents the status of SLAs as of September 2024.

Service-level agreement	Actual or expected date of signature	Total amount (EUR)	Duration	Counterpart	Short description
DG DIGIT	Signed	31,283.15	1 year (automatic renewal)	DIGIT	Global SLA for provision of IT services
DG HR	Signed	N/A	1 year (automatic renewal)	HR	SLA where DG HR provides implementation and operation of SYSPER and related services to ECCC
PMO	Signed	3,055.30	1 year (automatic renewal)	PMO	SLA for general assistance and/or provision of applications for which the PMO is system owner
EPSO	Signed	N/A	1 year (automatic renewal)	EPSO	SLA providing to ECCC assistance and access to Job oportunities page, reserve lists, EPSO's planning, ex-post controls, 3rd language testing and organisation of tailor made selections
EU Agencies Network	Signed	719.13	Indefinite period of time	SG	SLA to mutualise the costs for the Shared Support Office
ENISA	Signed	54,604.32	1 year (non automatic renewal)	ENISA	SLA for the provision of data protection officer services and accounting officer sercices. In adition a MoU was signed in 2023 between ENISA and ECCC.
DG BUDG	Signed	128,000.00	1 year (automatic renewal)	BUDG	SLA for implementation and usage of ABAC
eProcurement+Cloud Services	Signed	55,000.00	1 year (automatic renewal)	DIGIT	Amendment to SLA for access to eProcurement tool and Cloud Services
TESTA MoU	Signed	N/A	1 year (automatic renewal)	DIGIT	MoU for TESTA access/provision
CERT-EU	Signed	25,978.37	until end of year from signature - then 1 year renewal	DIGIT	SLA for the use of CERT-EU
SG	Ongoing	19,040.00	1 year (automatic renewal)	SG	Provision of HAN, ARES, Nomcom
CDT	Signed	4,002.00	1 year (automatic renewal)	CDT	transation services and editing
RTD	Signed	N/A	1 year (automatic renewal)	RTD	E Grants (EUR amount covered by CNECT in 2024)
Support of Expert management and Support services from REA	N/A	N/A	N/A	REA	No need for an SLA as we are under the mandate of REA

ANNEX XII. STRATEGY FOR COOPERATION WITH THIRD COUNTRIES AND/OR INTERNATIONAL ORGANISATIONS

To be updated in the future SPD.

ANNEX XIII: SPECIFICATIONS OF THE 'INCREASED CYBERSECURITY' CALL TO BE LAUNCHED BY ECCC IN ACCORDANCE WITH HORIZON EUROPE WORK PROGRAMME 2025

Destination - Increased Cybersecurity

[44] DECISION No GB/2024/8 of the European Cybersecurity Industrial, Technology and Research Competence Centre Governing Board on the Anti-Fraud Strategy 2024-2026 of the European Cybersecurity Competence Centre

The Horizon Europe strategic plan 2025-2027 identifies the following impact: "*Increased cybersecurity and a more secure online environment by developing and using effectively EU and Member States' capabilities in digital technologies supporting protection of data and networks aspiring to technological sovereignty in this field, while respecting privacy and other fundamental rights; this should contribute to secure services, processes and products, as well as to robust digital infrastructures capable to resist and counter cyber-attacks and hybrid threats".*

Expected impacts:

- Support the EU's technological capabilities by investing in cybersecurity research and innovation to further strengthen its leadership, strategic autonomy, digital sovereignty and resilience;
- Help protect its infrastructures and improve its ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from cyber and hybrid incidents, especially given the current context of geopolitical change;
- Support European competitiveness in cybersecurity and European strategic autonomy, by protecting EU products and digital supply chains, as well as critical EU services and infrastructures (both physical and digital) to ensure their robustness and continuity in the face of severe disruptions;
- Encourage the development of the European Cybersecurity Competence Community;
- Particular attention will be given to SMEs, who play a crucial role in the cybersecurity ecosystem and in overall EU digital single market competitiveness, by promoting security and privacy 'by design' in existing and emerging technologies.

Call - Increased Cybersecurity

HORIZON-CL3-2025-02-CS-ECCC

Conditions of the call[45]

Proposals are invited against the following topic(s):

Topics	Type of Action	Budgets (EUR million) 2025	Expected EU contribution per project (EUR million)[46]	Indicative number of projects expected to be funded
Opening: 12 Jun 2025 (tentative) Deadline(s): 12 Nov 2025 (tentative)				
HORIZON-CL3-2025-02-CS-ECCC-01: Generative AI for Cybersecurity applications	RIA	40.00	12.00 to 14.00	3
HORIZON-CL3-2025-02-CS-ECCC-02: New advanced tools and processes for Operational Cybersecurity	IA	23.55	4.50 to 6.00	4
HORIZON-CL3-2025-02-CS-ECCC-03: Privacy Enhancing Technologies	RIA	11.00	3.00 to 4.00	3
HORIZON-CL3-2025-02-CS-ECCC-04: Security evaluations of Post-Quantum Cryptography (PQC) primitives	RIA	4.00	2.00 to 3.00	2
HORIZON-CL3-2025-02-CS-ECCC-05: Security of implementations of Post-Quantum Cryptography algorithms	RIA	6.00	2.00 to 3.00	2
HORIZON-CL3-2025-02-CS-ECCC-06: Integration of Post-Quantum Cryptography (PQC) algorithms into high-level protocols	RIA	6.00	2.00 to 3.00	2
Overall indicative budget		90.55		

[45] The Executive Director-of the ECCC may decide to open the call up to one month prior to or after the envisaged date(s) of opening. The Executive Director of the ECCC may delay the deadline(s) by up to two months. All deadlines are at 17.00.00 Brussels local time. The budget amounts are subject to the availability of the appropriations provided for in the general budget of the Union for 2025.

[46] Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.

General conditions relating to this call	
Admissibility conditions	The conditions are described in General Annex A.
Eligibility conditions	The conditions are described in General Annex B.
Financial and operational capacity and exclusion	The criteria are described in General Annex C.
Award criteria	The criteria are described in General Annex D.
Documents	The documents are described in General Annex E.
Procedure	The procedure is described in General Annex F.
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G.

HORIZON-CL3-2025-02-ECCC-01: Generative AI for Cybersecurity applications

Call: Increased Cybersecurity	
Specific conditions	
Expected EU contribution per project	It is estimated that an EU contribution of between EUR 12.00 and 14.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 40.00 million.
Type of Action	Research and Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: In order to achieve the expected outcomes, and safeguard the Union's strategic assets, interests, autonomy, and security, participation in this topic is limited to legal entities established in Member States and Associated Countries. In order to guarantee the protection of the strategic interests of the Union and its Member States, entities established in an eligible country listed above, but which are directly or indirectly controlled by a non-eligible country or by a non-eligible country entity, shall not participate in the action.
Procedure	The procedure is described in General Annex F. The following exceptions apply: To ensure a balanced portfolio covering a broad range of research areas, grants will be awarded to applications not only in order of ranking but at least also to the two highest ranked proposal addressing expected outcome a) and the highest ranked proposal addressing expected outcome b), provided that the applications attain all thresholds.
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Impact: Action launched by the ECCC to incorporate 'expected impact' language set out in the 'Destination – Increased Cybersecurity' section of this work programme part.

Expected Outcome: Projects will develop technologies, tools, processes that reinforce cybersecurity using AI technological components, in particular Generative AI, in line with relevant EU policy, legal and ethical requirements.

Proposals should address at least one of the following expected outcomes:

a. Developing, training and testing of Generative AI models for monitoring, detection, response and self-healing capabilities in digital processes, and systems against cyberattacks, including adversarial AI attacks.

b. Development of Generative AI tools and technologies for continuous monitoring, compliance and automated remediation. These should consider legal aspects of EU and national regulation as well as ethical and privacy aspects.

Scope: The use of Artificial intelligence is becoming indispensable with applications where massive data is involved. Understanding all implications for cybersecurity requires deeper analysis and further research and innovation.

Generative AI presents both opportunities and challenges in the field of cybersecurity. This topic supports the research on new opportunities brought by Generative AI for Cybersecurity applications, to develop, train and test AI models to scale up detection of threats and vulnerabilities, enhance response time, cope with the large quantities of data involved, and automate process and decision-making support; for example by generating reports from threat

intelligence data, suggesting and writing detection rules, threat hunts, and queries for the Security information and event management (SIEM), creating management, audit and compliance reports and reverse engineering malware.

Proposals addressing expected outcome a)

(a) (i) Advanced threat and anomaly detection and analysis: Current cybersecurity tools may struggle to keep pace with the evolving tactics of cyber attackers. Developing, training and testing of Generative AI models can be used to analyse large volumes of data and accurately identify anomalies and deviations from normal patterns of behaviour, enabling more effective threat detection, analysis and response.

Tools should also support cybersecurity professionals as they may struggle to detect and respond to threats posed by generative AI, particularly as these systems become more sophisticated and difficult to distinguish from genuine human activity.

(a) (ii) Adaptive security measures: Cybersecurity tools often rely on static rules and signatures to detect threats, making them less effective against new and evolving attack methods. In addition, many cybersecurity tools still rely on manual intervention for threat response, which can be time-consuming and ineffective. Generative AI, through development, training, finetuning and testing of Generative AI models can support these tools to adapt and respond to emerging threats in real-time, improving overall security posture.

(a) (iii) Enhanced authentication and access control: The use of AI technologies could improve resilience of authentication and access control systems to unauthorized access and credential theft, making it more difficult for unauthorized users to gain access to sensitive information or systems.

Proposals addressing expected outcome b)

(b) (i) Development of tools powered by Generative AI that analyse and facilitate the Application of the national and EU regulation in digital systems, in particular the Artificial Intelligence Act, the Directive on measures for a high common level of cybersecurity across the Union (NIS2) and the Cyber Resilience Act.

(b) (ii) Adaptation to a dynamic environment. Companies, public sector and organisations face an ever-changing environment which makes keeping up with compliance towards cybersecurity rules challenging. On one hand there's a variety of rules applicable at sectorial, national or European level to be considered. On the other, change management and updates in ICT systems in organisations is frequent. Addressing both facets with tools powered with Generative AI brings the potential for a compliance continuum within organisations otherwise limited in time when driven by human intervention only.

All proposals are expected to respect Trustworthy and Responsible AI principles[47] and data privacy.

All proposals should demonstrate the EU added value by fostering the development of EU technology, the use of open-source technologies when technically and economically feasible, the exploitation of available EU data (Data Spaces, EOSC, federated data etc)

Proposals should define key performance indicators (KPI), with baseline targets to measure progress and to demonstrate how the proposed work will bring significant advancement to the state-of-the-art. All technologies and tools developed should be appropriately documented, to support take-up and replicability. Participation of SMEs is encouraged.

Proposals are expected to pay special attention to the Intellectual Property dimension of the results. The usability of the outcomes and results once the project is finished will be closely assessed.

[47] https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/guidelines-responsible-use-generative-ai-research-developed-european-research-area-forum-2024-03-20_en
https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

HORIZON-CL3-2025-02-CS-ECCC-02: New advanced tools and processes for Operational Cybersecurity

Call: Increased Cybersecurity	
Specific conditions	
Expected EU contribution per project	It is estimated that an EU contribution of between EUR 4.50 and 6.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 23.55 million.
Type of Action	Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: In order to achieve the expected outcomes, and safeguard the Union's strategic assets, interests, autonomy, and security, participation in this topic is limited to legal entities established in Member States and Associated Countries. In order to guarantee the protection of the strategic interests of the Union and its Member States, entities established in an eligible country listed above, but which are directly or indirectly controlled by a non-eligible country or by a non-eligible country entity, shall not participate in the action.
Technology Readiness Level	Tools and technologies developed are expected to start the project at minimum at TRL 4 and achieve at least TRL 7 by the end of the project – see General Annex B.
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G. The following exceptions apply: Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025)[48].
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Impact: Action launched by the ECCC to incorporate 'expected impact' language set out in the 'Destination – Increased Cybersecurity' section of this work programme part.

Expected Outcome: The use of and dependence on information and communication technologies have become fundamental aspects in all sectors of the economy. Public administrations, companies and citizens are more interconnected and interdependent across sectors and borders than ever before. This higher uptake of digital technologies increases exposure to cyber security incidents, vulnerabilities and their potential impacts. At the same time, Member States are facing growing cybersecurity risks and an overall complex threat landscape, with a clear risk of rapid spill-over of cyber incidents from one Member State to others.

Moreover, cyber operations are increasingly integrated in hybrid and warfare strategies, with significant effects on the target. In particular, the current geopolitical context is being accompanied by a strategy of hostile cyber operations, which is a game changer for the perception and assessment of the EU's collective cybersecurity crisis management preparedness and a call for urgent action. The threat of a possible large-scale incident causing significant disruption and damage to critical infrastructure and data spaces demands heightened preparedness at all levels of the EU's cybersecurity ecosystem. In recent years, the number of cyberattacks has increased dramatically, including supply chain attacks aiming at cyberespionage, ransomware, or disruption. The vulnerability landscape is also threatening. The ENISA Threat Landscape Report 2024[49] counts a total of 19,754 vulnerabilities. This amount of

[48] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

[49] The ENISA Threat Landscape Report 2024: ENISA Threat Landscape Report 2024: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

vulnerabilities can't be manually managed by humans. There is a need for automated management of vulnerabilities based on established standards like the Common Security Advisory Framework (CSAF)[50].

As regards detection of cyber threats and incidents, there is an urgent need to increase the exchange of information and improve our collective capabilities in order to reduce drastically the time needed to detect cyber threats and mitigate, before they can cause large-scale damage and costs. While many cybersecurity threats and incidents have a potential cross-border dimension, due to the interconnection of digital infrastructures, the sharing of relevant information among Member States remains limited. Proposals are expected to address this emerging threat landscape with the development of advanced frameworks, services tools, and processes, in line with relevant EU legislation (NIS2, Cyber Resilience Act, Cyber Solidarity Act).

Lastly, focus should be given to developing innovative frameworks, technologies, tools, processes, and services that reinforce cybersecurity capabilities for operational and technical cybersecurity cooperation, in line with relevant EU policy, with particular focus on NIS2, Cyber Solidarity Act and the EU Cybersecurity Strategy, as well as legal and ethical requirements.

Proposals should address at least two of the following expected outcomes:

- Enhanced Situational Awareness through advanced Cyber Threat Intelligence frameworks, tools, and services as well as cybersecurity risk assessments of critical supply chains made in the EU,
- Frameworks, tools, and services for preparedness against Cyber and Hybrid Threats in information and communication technology (ICT) and operational technology (OT), including cybersecurity exercises,
- Expanded Security Operations Centre/Computer Security Incident Response Teams (SOC/CSIRT) functionality through advanced tools and services for detection, analysis, incident handling including response and reporting as well as remediation,
- Development of testing and experimentation facilities for advanced tools and processes for operational cybersecurity, including the creation of digital twins for critical infrastructures and essential and important entities as defined in NIS2,
- Development and pilot implementation of cross-sector and/or cross-border cyber crisis management frameworks, services, and tools,
- Frameworks, services, and tools aimed at mechanisms and processes for enhanced operational cooperation between public sector entities (CSIRT network, EU-CyCLONe). Extension of the above to essential and important entities as defined in NIS2[51], would be an advantage.

Scope: Proposals are expected to demonstrate the developed frameworks, tools, services, and processes through pilot implementations involving the participation of relevant national cybersecurity authorities and/or essential and important entities as defined in NIS2, implemented with the participation of leading European cybersecurity industry. Proposals should consider the impact of forthcoming legislation, in particular the Cyber Resilience Act.

Real world applications and the usability of the solutions developed should feature predominately in the proposals.

The participation of the following types of entities is highly encouraged: innovative European cybersecurity start-ups and SMEs with a proven track-record in cybersecurity innovation at EU level (e.g. active participation in successful EU funded projects including cybersecurity projects under Horizon Europe, Digital Europe Programme cybersecurity projects or EIC Pathfinder or Accelerator projects), European start-ups and SMEs that can demonstrate established operational cooperation with relevant National Cybersecurity Authorities, European start-ups and SMEs that have received equity investments by national, European or private Venture Capital funds for cybersecurity activities etc.

[50] Common Security Advisory Framework (CSAF): https://csaf.io/

[51] Directive on measures for a high common level of cybersecurity across the Union: https://eur-lex.europa.eu/eli/dir/2022/2555

The participation of these start-ups and SMEs with an active role in the implementation of the proposed action (project coordination, technical coordination, lead of pilot implementation etc) would be considered an asset.

HORIZON-CL3-2025-02-CS-ECCC-03: Privacy Enhancing Technologies

Call: Increased Cybersecurity	
Specific conditions	
Expected EU contribution per project	It is estimated that an EU contribution of between EUR 3.00 and 4.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 11.00 million.
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: subject to restrictions for the protection of European communication networks.
Type of Action	Research and Innovation Actions
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G. The following exceptions apply: Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025)[52].
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Impact: Action launched by the ECCC to incorporate 'expected impact' language set out in the 'Destination – Increased Cybersecurity' section of this work programme part

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Development of robust, scalable, and reliable technologies to uphold privacy within federated and secure data sharing frameworks, as well as in the processing of personal and industrial data, integrated into real-world systems.
- Development of privacy preserving approaches for data sharing solutions, including privacy-preserving cyber threat information sharing, and in collaborative computations involving sensitive data.
- Integration of privacy-by-design at the core of software and protocol development processes, with attention to ensure that cryptographic building blocks and implementations of privacy-enhancing digital signatures and user-authentication schemes are crypto-agile and modular, to facilitate a transition towards post-quantum cryptographic algorithms.
- Development of privacy enhancing technologies for the users of constrained devices.
- Contribution towards the advancement of GDPR-compliant European data spaces for digital services and research, such as those on health data, aligning with DATA Topics of Horizon Europe Cluster 4.
- Development of privacy enhancing technologies and solutions, to benefit the requirements of citizens and companies, including small and medium-sized enterprises (SMEs).
- Development of blockchain-based and decentralized privacy-enhancing technologies, to preserve data confidentiality, integrity, and the authenticity of transactions and digital assets. Possible combination of blockchain with other technologies, such as federated learning, will need to address the data's security and privacy shared through such networks while ensuring that their connected devices are trusted.
- Investigating the usability and user experience of privacy-enhancing technologies and exploring ways to design systems that are both secure and user-friendly.

[52] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

Scope: Protecting individuals' personal data and ensuring privacy while allowing for data processing and analysis is fundamental for our society. Privacy-preserving techniques allow to minimize the amount of personal data collected and processed, and to protect that data through advanced cryptographic methods. For instance, machine-learning methodologies are leveraged to dissect medical and behavioural data, aiming to unearth causations and insights into cyber attacks or threats. However, a substantial portion of this data comprises personal information, (such as sensitive health data), raising concerns over potential breaches or misuse, thus jeopardizing the privacy of individuals, societal well-being, and economic stability.

In addition, the challenges related to the exploitation of non-personal/industrial data assets, which could impede the full realization of the data-driven economy, are also subject to the work that can be proposed under this topic. Solutions that can provide security against quantum adversaries are also encouraged.

Privacy-enhancing technologies (PETs) such as cryptographic anonymous credentials, differential privacy, secure multiparty computation, homomorphic encryption, advanced digital signatures, such as ring signatures, blind signatures and attribute-based credentials hold promise in mitigating these challenges, yet their practical application necessitates further refinement and rigorous testing. Consortia are encouraged to propose solutions that can improve the usability and effectiveness of different PETs in realistic environment and to investigate their integration within common European data spaces. The inclusion of agile schemes designed in a modular way to support the transition to post-quantum PETs and the design, improvement and security analysis of quantum-resistant PETs is welcome, in light of the advances of quantum technologies.

Proposals should also focus on enhancing the usability, scalability, and dependability of secure and PETs within supply chains, while seamlessly integrating with existing infrastructures and conventional security protocols. They should also accommodate the diversity in data types and models across various organizations, undergoing validation and pilot runs within authentic data environments. Adherence to data regulations, notably GDPR, is paramount.

Consortia should seek to intertwine interdisciplinary expertise and resources from industry stakeholders, service providers, and end-users. The engagement of SMEs is encouraged, alongside the inclusion of legal proficiency to ensure regulatory compliance, including GDPR adherence. Furthermore, proactive identification and assessment of potential regulatory hurdles and constraints for the developed technologies/solutions are strongly encouraged.

HORIZON-CL3-2025-02-CS-ECCC-04: Security evaluations of Post-Quantum Cryptography (PQC) primitives

Call: Increased Cybersecurity	
Specific conditions	
Expected EU contribution per project	It is estimated that an EU contribution of between EUR 2.00 and 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 4.00 million.
Type of Action	Research and Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: In order to achieve the expected outcomes, and safeguard the Union's strategic assets, interests, autonomy, and security, participation in this topic is limited to legal entities established in Member States and Associated Countries and OECD countries. In order to guarantee the protection of the strategic interests of the Union and its Member States, entities established in an eligible country listed above, but which are directly or indirectly controlled by a non-eligible country or by a non-eligible country entity, shall not participate in the action.
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G. The following exceptions apply: Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation

	(2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025)[53].
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Impact: Action launched by the ECCC to incorporate 'expected impact' language set out in the 'Destination – Increased Cybersecurity' section of this work programme part

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Breakthroughs in understanding the quantum hardness of various mathematical problem classes that underpin the security of current and future post-quantum cryptosystems;
- New quantum algorithms with significant quantum speed-up for lattice-based, code-based, and potentially other mathematical problem-classes;
- Improved implementation of quantum algorithms using high-level quantum programming languages to solve mathematical problems forming the core of cryptosystems;
- Establishment of environments testing the robustness of cryptosystems regarding quantum attackers;
- AI-based approaches to help discovering vulnerabilities of lattice-based or other mathematical problem-classes;
- Cryptanalysis results;
- Parameter suggestions to create a robust set of cryptographic building blocks for post-quantum cybersecurity and design of post-quantum cryptosystems with improved security against quantum or AI-based attacks.

Scope: The intrinsic security of PQC algorithms is based on mathematical problems that are believed to be intractable for both classical and quantum computers. To assess the quantum security of post-quantum primitives is fundamental in order to boost our confidence on post-quantum cryptosystems. The development of quantum algorithms demonstrating a significant quantum speed-up would represent a major breakthrough, necessitating a reassessment of the security of cryptosystems (lattice-based, code-based, and others). Conversely, if no significant quantum speed-up is discovered, it would bolster our confidence in the security of these post-quantum cryptosystems, though some parameters may still require fine-tuning. Moreover, up to now existing quantum attackers have been analyzed mostly in a theoretical way. However, their application to nowadays cryptosystems fail due to a lack of efficient implementations and hardware. Studies are also needed on AI-based approaches that may be used to attack certain schemes with certain implementation choices, and the discovery of eventual vulnerabilities can help the research community develop more robust post-quantum cryptosystems.

Proposals on the assessment of the security of post-quantum primitives, via studies focused on eventual quantum algorithms with demonstrable speed-up, eventually also in combination with AI, or on solely AI-based approaches, are welcome. The security of lattice and code-based PQC algorithms may be prioritized, but tackling other mathematical problem classes is not excluded. As the unprecedented computational power of quantum computing can greatly enhance AI capabilities, combination of different approaches may also be considered. Consortia with team of applicants with background in post-quantum cryptography and in quantum computing are particularly encouraged. Projects should lead to identification of vulnerabilities of current post-quantum cryptographic building blocks and to practical recommendations for parameters for the design of post-quantum cryptosystems with improved security against quantum attacks and future advances in code-breaking and AI.

[53] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

HORIZON-CL3-2025-02-CS-ECCC-05: Security of implementations of Post-Quantum Cryptography algorithms

Call: Increased Cybersecurity	
Specific conditions	
Expected EU contribution per project	It is estimated that an EU contribution of between EUR 2.00 and 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 6.00 million.
Type of Action	Research and Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: In order to achieve the expected outcomes, and safeguard the Union's strategic assets, interests, autonomy, and security, participation in this topic is limited to legal entities established in Member States and Associated Countries and OECD countries. In order to guarantee the protection of the strategic interests of the Union and its Member States, entities established in an eligible country listed above, but which are directly or indirectly controlled by a non-eligible country or by a non-eligible country entity, shall not participate in the action.
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G. The following exceptions apply: Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025)[54].
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Impact: Action launched by the ECCC to incorporate 'expected impact' language set out in the 'Destination – Increased Cybersecurity' section of this work programme part

Expected Outcome: Projects' results are expected to contribute to some or all of the following outcomes:

- Design and implementations of Post-Quantum Cryptography (PQC) algorithms that are resistant to side-channel and fault attacks;
- Optimized countermeasures taking into account a balanced trade-off between security, performance, and costs;
- Recommendations on implementing countermeasures for a broad range of attacks, also identifying the available and necessary hardware;
- Analysis of new attacks or combinations of attacks, also eventually enhanced by AI, applicable to real-world conditions.
- Design of automated security evaluations for PQC implementations.

Scope: The security of the implementations of PQC algorithms is vital for maintaining the confidentiality, integrity, authenticity and availability of digital information and communications in the face of implementation attacks, such as, for example, side-channel attacks using information from timing, power consumption, electromagnetic radiation, fault attacks disturbing the secure of operation of the device and their combination. Such attacks, eventually also enhanced by the use of deep learning, constitute significant threats to both (embedded and regular) software and hardware implementations. In various application areas such as IoT, cloud-based applications, automotive, measures to prevent such attacks currently lead to substantial resource overhead due to the complexity of the algorithms, and the security remains unclear given the limited exploration of different attack surfaces. Countermeasures, to the extent that they are available, may have significant impact on run-time and memory consumption. Resistance in PQC

[54] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

implementations to implementation attacks is an increasingly common concern among customers, especially when exploring the right balance between security and performance.

Evaluating the security of PQC algorithm implementations against side-channel and fault attacks is crucial, given the proven vulnerabilities. Various countermeasures, such as masking, shuffling, randomized clocking, random delay insertion, constant weight encoding, code polymorphism, control-flow integrity and re-computation of critical operations can be employed to mitigate these attacks. Synergies between specific countermeasures and the design of cryptographic systems are available for pre-quantum cryptography but require investigation for post-quantum cryptography.

Proposals are welcome on developing solutions that protect against such implementation attacks, at reasonable costs and minimizing the loss of performance while maintaining the required security, as well as on the analysis of new attacks or combinations of attacks, also powered by the use of AI, for security-by-design approaches when designing Post Quantum Cryptographic systems. Activities can also lead to the development of testing methodologies and frameworks for automated security evaluations for correctness and resistance to remote side-channel attacks for regular software and for correctness and resistance to a broad range of implementation attacks for embedded software and hardware.

HORIZON-CL3-2025-02-CS-ECCC-06: Integration of Post-Quantum Cryptography (PQC) algorithms into high-level protocols

Call: Increased Cybersecurity	
Specific conditions	
Expected EU contribution per project	It is estimated that an EU contribution of between EUR 2.00 and 3.00 million would allow these outcomes to be addressed appropriately. Nonetheless, this does not preclude submission and selection of a proposal requesting different amounts.
Indicative budget	The total indicative budget for the topic is EUR 6.00 million.
Type of Action	Research and Innovation Actions
Eligibility conditions	The conditions are described in General Annex B. The following exceptions apply: In order to achieve the expected outcomes, and safeguard the Union's strategic assets, interests, autonomy, and security, participation in this topic is limited to legal entities established in Member States and Associated Countries and OECD countries. In order to guarantee the protection of the strategic interests of the Union and its Member States, entities established in an eligible country listed above, but which are directly or indirectly controlled by a non-eligible country or by a non-eligible country entity, shall not participate in the action.
Legal and financial set-up of the Grant Agreements	The rules are described in General Annex G. The following exceptions apply: Eligible costs will take the form of a lump sum as defined in the Decision of 7 July 2021 authorising the use of lump sum contributions under the Horizon Europe Programme – the Framework Programme for Research and Innovation (2021-2027) – and in actions under the Research and Training Programme of the European Atomic Energy Community (2021-2025)[55].
Security Sensitive Topics	Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN). Please refer to the related provisions in section B Security — EU classified and sensitive information of the General Annexes.

Expected Impact: Action launched by the ECCC to incorporate 'expected impact' language set out in the 'Destination – Increased Cybersecurity' section of this work programme part

Expected Outcome: Proposals are expected to contribute to some or all of the following outcomes:

[55] This decision is available on the Funding and Tenders Portal, in the reference documents section for Horizon Europe, under 'Simplified costs decisions' or through this link: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ls-decision_he_en.pdf

- Design and implementations of at least one high-level post-quantum cryptography protocol along with a security analysis demonstrating that no security is lost compared to the used building blocks/lower-level protocols (KEMs, signatures, AEAD, ...);
- Submission of these high-level protocols integrating PQC to standardization bodies and/or submission of the specification and implementation to the respective open source projects;
- Requirements analysis highlighting roadblocks and needs for development of PQC solutions for missing building blocks for migrating high-level protocols to PQC.

Scope: The transition to post-quantum cryptography requires changing the uses of most currently deployed public-key cryptography (RSA and ECC). Research and development efforts are providing signature systems and key-exchange mechanisms that are generally accepted to withstand attacks using classical and quantum computers. Efforts are on the way to include these in core Internet protocols such as Transport Layer Security (TLS). While this is an important development, many more protocols need to be modified to be quantum-ready and to ensure backward compatibility with legacy systems. Various application areas, such as Internet of Things, cloud-based applications, and automotive, place constraints on bandwidth or processing time which may prompt different choices than those employed for TLS. Currently used high-level protocols may have components that are specific to Elliptic Curve Cryptography (ECC) or to Rivest-Shamir-Adleman (RSA) or may require additional building blocks next to or in place of signatures and key-exchange mechanisms. While applications that provide authenticity are less urgent to migrate than those for confidentiality, those using embedded hardware such as secure elements, Two-Factor Authentication (2FA) and Multi-Factor Authentication (MFA) using hardware tokens and others have a very slow turnover and need to be replaced by the time large quantum computers exist, thus requiring migrating the design in the near future.

Activities should target one or multiple relevant high-level protocols and produce their post-quantum versions. Typically, this can be achieved through combining current and post-quantum solutions for backward compatibility. Atypical solutions with equivalent security are also welcome. Consortia composed by actors of different nature, such as, for example, research institutions, relevant public entities, and industry to ensure that PQC solutions meet real-world security demands and are robustly tested across various applications are also welcome.