DECISION No GB/2026/1

of

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

Adopting the Single Programming Document 2026-2028

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) 2019/715[2] applies to the ECCC;

Having regard to Commission Communication C(2020) 2297 final, 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 dated on 20 April 2020;

Having regard to Article 30 of the ECCC Governing Board Decision No GB/2024/3 on the Revision of DECISION No GB/2023/1 on the ECCC's Financial Rules;

HAS ADOPTED THE FOLLOWING DECISION:

Article 1

The Single Programming Document 2026-2028 is adopted as set out in the Annex 1 of this decision.

[1] OJ L 202, 8.6.2021, p. 1-31

[2] Commission Delegated Regulation (EU) 2019/715 of 18 December 2018 on the framework financial regulation for the bodies set up under the TFEU and Euratom Treaty and referred to in Article 70 of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council (OJ L 122, 10.5.2019, p. 1)

Article 2

The Statement of estimates for the financial year 2026 is adopted as part of SPD financial annexes of this Decision.

The Single Programming Document, including the 2026 work programme and statements of estimates for 2026, shall become definitive after the final adoption of the General Budget of the European Union for 2026. In the event of a change in the amount of the European Union contribution and/or in the establishment plan, the respective provisions of the work programme shall be adjusted accordingly.

Article 3

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

Done at Bucharest on 9 January 2026,

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 2026-2028

Version adopted by the ECCC GB Decision 2026/1

CONTACT

To contact the European Cybersecurity Competence Centre (ECCC) or for general enquiries, please use:
Email address: info@eccc.europa.eu
https://cybersecurity-centre.europa.eu/index_en

LEGAL NOTICE

This publication presents the final ECCC Single Programming Document (SPD) 2026-2028 as adopted by the Governing Board of the ECCC in Decision No GB/2026/1. It builds on the Draft ECCC Single Programming Document (SPD) 2026-2028 as approved by the Governing Board of the ECCC in Decision No GB/2025/1. The Governing Board may amend the Single Programming Document 2026–2028 at any time. The ECCC has the right to alter, update or remove the publication or any of its contents.

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

TABLE OF 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. 2025 will be the year when the setup stage of the ECCC will be complete. The ECCC will be on cruising speed, fully operational, coordinating and managing calls under the Horizon Europe and Digital Europe programmes (HEP, DEP), and fostering cooperation of the Cybersecurity Competence Community (the Community).

The activities of the ECCC are part of the EU systematic efforts to strengthen its cybersecurity posture. In recent years, the EU has continued developing its cybersecurity policy. This includes, among others, the NIS 2 Directive, the amendment of Cybersecurity Act (CSA), the new Cyber Resilience Act (CRA) and the Digital Operational Resilience Act (DORA), the Cyber Solidarity Act (CSoA), the Communications on the Cybersecurity Skills Academy and on cyber defence as well as the European action plan on the cybersecurity of hospitals and healthcare providers and the European action plan on cables security. ECCC has a significant role in implementing the legislation, financing beneficiaries to implement these initiatives through DEP and HEP.

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 the multiannual planning 2026-2028 and the work programme for 2026. The objective is to have its final version adopted by the ECCC GB at the beginning of 2026. 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. The document will be updated with the allocations and the topics foreseen in the future ECCC Cybersecurity DEP WP 2025-2027 amendment during Q1/2026 while the budget includes HEP WP contribution foreseen for 2026[1].

In 2026 the ECCC will build-up on the results of the hard work from previous years and the engagement of all those who contributed to the set-up of the ECCC, including ECCC staff, European Commission (EC), members of the ECCC GB, the Network of NCCs and many others in the Cyber Competence Community. The vision of the ECCC regulation will progressively materialise, demonstrating the added value of the EU strategic investments and enhanced coordination in cybersecurity.

December 2025

Luca Tagliaretti

[1] European Commission Decision C(2025) 8493 of 11 December 2025, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=intcom:C%282025%298493

LIST OF ACRONYMS

ABAC	Accrual-based accounting
AD	Administrator
AST	Assistant
CA	Contract agent
CERT-EU	Computer Emergency Response Team for the EU institutions, bodies and agencies
CRA	The Cyber Resilience Act
CSA	The Cybersecurity Act
CSoA	The Cyber Solidarity Act
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
DEP	Digital Europe Programme
DORA	Digital Operational Resilience Act
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
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
PAD	Public Access to Documents
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
WP	Work Programme

MISSION STATEMENT

The European Cybersecurity Competence Centre (ECCC)[2] is a European Union (EU) body established by Regulation (EU) 2021/887[3] 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)[4], the Horizon Europe Program (HEP)[5], 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[6] 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.
- 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:

[2] https://cybersecurity-centre.europa.eu/index_en.
[3] Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (OJ L 202, 8.6.2021, p. 1).
[4] 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).
[5] 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).
[6] 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

- 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*"[7] 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*"[8], 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[9], 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[10] 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. A prompt reaction to this call for action resulted in the EU Action Plan on Cable Security[11] which foresees the support to preparedness testing/stress testing of communication cables through the Cyber Solidarity Act under DEP.

Such initiatives echo the EU's ambition for a common situational awareness and coordinated preparation and response to threats. A priority area of focus 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). The NIS 2 Directive[12] provides a legal basis for the EU-CyCLONe, the network of MS cyber crisis management authorities plus, in case of a potential or ongoing large-scale cybersecurity incident that has or is likely to have a significant impact on services and activities falling within the scope of the NIS2 Directive[13], for the EC to participate in crisis management coordination and situational awareness.

[7] Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade, JOIN/2020/18 final.
[8] Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade (6722/21).
[9] 'Nevers Call to Reinforce the EU's Cybersecurity Capabilities'. Informal Meeting of the Telecommunications Ministers. Nevers, March 9, 2022.
[10] https://www.consilium.europa.eu/en/press/press-releases/2022/05/23/cyber-posture-council-approves-conclusions/
[11] Joint Communication to the European Parliament and the Council: EU Action Plan on Cable Security, JOIN/2025/ 9 final
[12] Directive 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
[13] See please NIS 2 Directive, Article 16(2)

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

- **NIS 2 Directive (NIS 2).** To respond to the increased exposure of Europe to cyber threats, a revised of the NIS Directive (NIS 2 Directive) entered into force in January 2023 with the national transposition measures to be applied as from 18 October 2024. The NIS 2 Directive raises the EU common level of ambition on cyber-security, through a wider scope, clearer rules and stronger supervision tools.
- **Cyber Resilience Act (CRA).** In September 2022, the EC presented the proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements, which shall apply as of 10 December 2027 (Cyber Resilience Act, CRA)[14]. 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.
- **Cyber Solidarity Act.** The Cyber Solidarity Act[15], which entered into force on February 4,2025 is 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 complements ECCC actions to provide long-term solutions to strengthen solidarity at Union level. 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.** Regulation (EU) 2023/2841 which entered into force in December 2023, 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.
- **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 is applicable while three 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) and the cybersecurity certification scheme for EU Digital Identity (EUDI) Wallets. In support of certification, the EU Standardisation Strategy and the current EU funding framework both include essential topics such as the development of harmonised evaluation methodologies or promoting innovations to the performance of testing ICT products, services and processes.

[14] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), OJ L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj

[15] Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act), OJ L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj

[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).

- **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. The EC adopted a Communication on this topic in June 2023[18], 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[19] at large and identified a number of key threats that could pose significant risks for the security and resilience of the connectivity infrastructure. Member States, the EC and ENISA are working on the implementation of the recommended measures to mitigate these risks.
- **EU funding in the 2021-2027 Multiannual Financial Framework.** For the previous years, funding was provided for projects on cybersecurity deployment under the DEP, and for cybersecurity research under the HEP, while further funding is foreseen for the current and coming years under both EU programmes as per the related adopted Work Programmes, to a large extend channelled through ECCC.
- **EU Cybersecurity Skills Academy.** The Commission continues implementing the communication on a Cybersecurity Skills Academy, launched in 2024. In this regard, NCCs are being consulted or kept informed of developments relating repositories of trainings and certifications, pilots on an attestation scheme for cybersecurity skills, the definition of indicators to evaluate the workforce in the EU, the European Cybersecurity Skills Framework, pledges and the Industry-Academia Network.
- **EU Cyber Defence Policy**. The EU Policy on Cyber Defence has been set out in a Joint Communication from the Commission and the High Representative in 2022[20]. It was welcomed by Council Conclusions in 2023[21] which include references to the ECCC as an essential pillar to support the scale up of European cybersecurity industry.

  In this context, the **Action plan on synergies between civil, defence and space industries**[22] is also relevant considering the aim to enhance the complementarity between relevant EU programmes and instruments covering research, development and deployment and to create synergies.
- **European action plan on the cybersecurity of hospitals and healthcare providers**[23]**:** In January 2025, the European Commission launched a comprehensive action plan to improve the cybersecurity of hospitals and healthcare providers across the EU. As healthcare systems increasingly become targets of cyber and ransomware attacks, this plan aims to strengthen the security of the European health systems. This is a priority initiative for the new Commission, which was announced by President von der Leyen in her Political Guidelines. The Action Plan takes a holistic approach, focusing on preparedness, detection, response, recovery and deterrence. Through the Action Plan, the cybersecurity framework that the EU has developed in the past years is operationalised, to deliver concrete results for the healthcare sector.
- **AI Continent Action Plan**[24]: As set out by President von der Leyen at the AI Action Summit in February 2025 in Paris, this ambitious Action Plan, published in April 2025, is set to transform Europe's strong traditional industries and its exceptional talent pool into powerful engines of AI innovation and acceleration. This initiative will boost the European Union's AI innovation capabilities through actions and policies around five key pillars: (1) Building a large-scale AI data and computing infrastructure, (2) Increasing access to large and high-quality data, (3) Developing algorithms and fostering AI adoption in strategic EU sectors (4) Strengthening AI skills and talents (5)

[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] European Commission, Implementation of the 5G cybersecurity Toolbox, C(2023)4049 final, 15 June 2023.
[19] 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
[20] Joint Communication to the European Parliament and the Council: EU Policy on Cyber Defence, JOIN(2022)49 final, 10 November 2022.
[21] The Council Conclusions on the EU Policy on Cyber Defence, as approved by the Council at its meeting held on 22 May 2023, available at: https://www.consilium.europa.eu/media/64526/st09618-en23.pdf
[22] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - Action Plan on synergies between civil, defence and space industries, COM(2021) 70 final)
[23] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions- European action plan on the cybersecurity of hospitals and healthcare providers, COM(2025) 10 final
[24] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions- AI continent Action Plan, COM(2025) 165 final

Regulatory simplification. Leveraging cutting-edge technologies like AI or quantum, can build a resilient cybersecurity landscape that serves and protects everyone.

- In addition, the ECCC should strengthen its collaboration with strategic initiatives of the Commission, such as in Artificial Intelligence (AI), High Performance Computing (HPC) and Quantum Computing and related stakeholders.
- **Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography**[25]**:** This Commission Recommendation encourages Member States to develop a comprehensive strategy for the adoption and deployment of Post-Quantum Cryptography, to ensure a coordinated and synchronised transition among the different Member States and their public sectors and critical infrastructures across the whole EU.
- The **EU Action Plan on Cable Security**[26] presented by the EC and the High representative which foresees the support to preparedness testing/stress testing of communication cables through the Cyber Solidarity Act under DEP.

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.

The ECCC, 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 duplication of effort and resources.

[25] COMMISSION RECOMMENDATION of 11.4.2024 on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography, C(2024) 2393 final
[26] Joint Communication to the European Parliament and the Council: EU Action Plan on Cable Security, JOIN/2025/ 9 final

SECTION II. MULTI-ANNUAL PROGRAMMING 2026 – 2028

The ECCC, in consultation with its GB, developed a multi-annual programming covering three years. The structure of the SPD is aligned with the way ECCC should implement its tasks, as described in Article 4(3) of ECCC regulation.

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 multi-annual 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 paragraphs (a) and (c) of Article 4(3) of the ECCC Regulation. One more horizontal/cross cutting activity: Activity 3, to support the governance and 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 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	√	√	

ECCC tasks and responsibilities	Activity 1	Activity 2	Activity 3
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		√	

II.1 MULTI-ANNUAL WORK PROGRAMME

The Activities for the Multiannual Work Programme 2026-2028 of the ECCC correspond to three specific objectives:

- **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 3-year period 2025-27 is approximately EUR 355 million.

  The adoption of the ECCC DEP cybersecurity work programme 2025-2027 by the ECCC was a major milestone. Key tasks will be the evaluation of DEP calls for proposals, preparation and signature of grants and procurements, and managing projects. The ECCC will entirely manage these tasks, as well as existing cybersecurity DEP projects, independently from EC services, having reached 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 some of the HEP projects[27] 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**

[27] Commission Implementing Decision C/2025/8493 final from December 2025 on the financing of the Specific Programme implementing Horizon Europe – the Framework Programme for Research and Innovation – and the adoption of the work programme for 2026-2027

The ECCC will facilitate and coordinate the work of the Network of NCCs, in particular by facilitating the works of the ECCC GB Working Groups and their Chairs as secretariat. The Network is composed of one NCC from each MS[28]. 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 during the meeting in June:

- WG 1: Community Building (successor of WGs 1 and 3)
- WG 2: Boost application process success
- WG 3: International awareness (successor of WG6)
- WG 4: Strategic advice (successor of WG 4)
- WG 5: Cyber skills (successor of WG 5)
- WG 6: Cyber Hubs (successor of WG 7)

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[29] 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[30], 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):

- *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.*

[28] 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.
[29] 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.
[30] Article 2 point (8) of the Regulation

- *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**

Having completed its establishment phase, the ECCC is focused on unlocking its full organizational potential. It is committed to the principles of sound financial management, performance effectiveness, and full budget transparency, ensuring all resources are managed for maximum impact and accountability. By integrating people, processes, technology, and culture, the ECCC will become a sustainable, resilient, and long-lasting organization, and position itself as an employer of choice.

Strategic Governance and Sustainability. The ECCC's organisational strategy is built on a strong governance framework that promotes efficient and consistent management through planning, reporting, and coordination. Proactive risk management, clear communication, and active stakeholder engagement ensure transparency and trust. The Centre maintains close ties with its Governing Board and adapts working groups to align with strategic priorities.

Policies and control mechanisms. ECCC's policies and control mechanisms are designed to ensure strict compliance with its legal and regulatory framework. The organisation continuously supervises, adjusts, and improves its internal control systems, workflows, and standard procedures to promote transparency, accountability, and to ensure effective decision-making. These policies underpin managerial oversight, facilitate proper information flow, and strengthen control structures, addressing potential internal control deficiencies identified through risk assessments, audit recommendations, and compliance reviews.

The internal control system is supported by regular reviews and updates of procedures, ensuring sound financial management, fraud prevention, and risk mitigation. Effective coordination with the governance bodies ensures clear communication, stakeholder engagement, and adherence to international standards, maintaining the integrity and resilience of ECCC's operations.

People and Talent Development. ECCC's People and Talent Development focuses on aligning financial and human resources to meet evolving stakeholder needs efficiently. Recruitment and retention strategies are under development and will be continuously improved to attract top talent, shorten hiring times, and ensure a positive candidate experience through a modernised careers website and competency-based HR management. Accountability is strengthened through clear definition or roles and responsibilities.

Ongoing learning, professional growth, and well-being are prioritised to build a resilient workforce with the right skills at the right time and place. Leadership development and a strong culture of engagement, inclusion, and ethics underpin the organisation's values and drive.

Optimisation and digital workplace. ECCC is committed to enhancing operational excellence by adopting Lean management principles and automating routine workflows, enabling faster, more agile, and higher-quality services that ensure transparency, efficiency and sound financial management.

In the realm of technology and digital workplace, ECCC aims to expand collaborative platforms, further explore the use of AI, decentralised access, and cloud solutions to support hybrid work and improve information flow. Real-time dashboards for HR, budget, and project metrics will enable leaders to make swift, informed decisions and reporting.

Environmental sustainability and social responsibility. The ECCC is committed to integrating environmental and climate considerations across all operations, carefully assessing the impact of its power consumption, waste, and material use. The Centre aims to develop a robust environmental management system and pursue Eco-Management and Audit Scheme (EMAS) certification.

Facilities and resource management uphold rigorous standards for health, safety, and ergonomics, ensuring full policy compliance. Sustainability efforts focus on energy saving, workplace safety, and ergonomics, targeting full adherence to relevant policies.

Furthermore, the ECCC staff community actively engages in initiatives that strengthen internal cohesion and contribute to the local community through volunteering and social responsibility events, reinforcing the Centre's commitment to sustainable and responsible organisational growth.

Cooperation agreements with EU agencies. ECCC's cooperation agreements with EU agencies/institutions and other partners are founded on a framework of collaboration, formalised through existing agreements, work programmes, and operational projects. The Centre actively aligns its activities with other EU Agencies to foster synergies, exchange expertise, and coordinate efforts on cybersecurity initiatives.

Regular updates on these cooperation efforts are provided to the Governing Board, ensuring alignment with strategic objectives. The focus remains on multi-stakeholder engagement, including industry, academia, and NCCs, to build a shared cybersecurity ecosystem that fosters innovation and resilience across Europe.

II.2 HUMAN AND FINANCIAL RESOURCES - OUTLOOK FOR YEARS 2026 – 2028

The ECCC Regulation entered into force on 28 June 2021. Most staff joined in 2023, followed by the appointment of the Executive Director in 2024 and the management team in 2025. By 2025, the ECCC had established its initial structure and implemented regular assessments of resource allocation to address growing demands, optimising both financial and human resources. The 2026–2028 multiannual programme builds on these efforts, focusing on enhanced agility and operational efficiency through effective use of allocated resources.

II.2.1 Overview of the past and current situation

As of 31 December 2025, the ECCC's overall staff occupancy rate stands at 87%. Two Contract Agents and one Administrator are currently in the onboarding process, having accepted offers or undergoing medical examinations. The selection process for Seconded National Experts has concluded, with follow-up interviews underway. Full staffing is anticipated shortly, with the exception of one remaining Administrator position.

II.2.2 Outlook for the years 2026 – 2028

As of Q4/2024 and its achieved financial autonomy the ECCC has taken over all activities and tasks within the ECCC mandate in the implementation and management of DEP and HEP. In addition, the ECCC is providing strategic advice and coordination on cybersecurity related topics, including the support for Working Groups and the functioning of the NCC Network and Strategic Advisory Group which is setup early 2026.

After reaching full operational capacity in 2026, the ECCC will enter a steady operational phase, equipped to deliver on its assigned mandate. The Centre will transition into a mature organisation with stable human and financial resources. It will continue to deepen its core activities, particularly in facilitating access to funding programmes related to cybersecurity and services for the Cybersecurity Community by implementing the Strategic Agenda, calls for grants, implementing join procurements, coordinating the Network of National Coordination Centres (NCCs), ATLAS and enhancing cooperation among relevant authorities.

The ECCC will continue evolving as a fully operational organisation dedicated to delivering high-quality services to its stakeholders. Its organisational development will prioritise talent management and workforce planning, focusing on the effective growth and deployment of its resources to meet evolving challenges and sustain operational excellence.

II.2.3 Resource programming for the years 2026 – 2028

Financial Resources

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.

Annex II provides a detailed overview of ECCC's operational expenditure, whereas Annex III breaks down the budget according to ECCC's budgetary structure that groups operational expenditures. 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.

Human Resources

The Staff Regulations and Conditions of Employment of Other Servants of the EU apply to the staff of the ECCC. The human resource estimations for the 2026-2028 period are based on adopted regulations. Two new posts are foreseen for 2026, as detailed in consolidated amendment[31] for the budget of 2026. For further info please see Annex IV.

II.2.4 Strategy for achieving efficiency gains

The European Cybersecurity Competence Centre (ECCC) is advancing a comprehensive agenda of digital transformation, agility, governance improvements, and cross-agency cooperation to reinforce its role as a forward-looking EU body. The ECCC's strategy rests on a combination of technology, people, and culture to deliver efficiency, agility, and long-term impact.

Digital Transformation and Process Automation. The ECCC will scale up successful AI pilots to streamline repetitive tasks such as automated reporting, document review, stakeholder support, and knowledge extraction. In parallel, IT tools will be deployed to simplify routine administrative activities like planning, budgeting, recruitment, and HR onboarding. A stronger focus will also be placed on automating cross-system workflows by integrating core platforms such as ARES, Anaplan, Power BI, and Microsoft 365, ensuring seamless data flows and eliminating double data entry. Complementing this, paperless processes will be enhanced through e-signature solutions and digital archiving, accelerating decisions while lowering costs and administrative burdens.

Workforce Agility and Resource Optimisation. To ensure sustainable and strategically aligned expertise, the European Cybersecurity Competence Centre (ECCC) will refine its organisational structure to proactively address future responsibilities and optimise resource utilisation. It will also map the expertise of its staff. By balancing internal expertise with targeted external support, the ECCC aims to reduce reliance on contractors and strengthen in-house

[31] Please see page 45, https://data.consilium.europa.eu/doc/document/ST-15487-2025-ADD-5/en/pdf

capabilities. Ongoing upskilling initiatives will equip staff with essential digital competencies, including AI literacy, project management, data analytics, and agile methodologies - enabling effective use of new tools in daily operations.

Governance and Planning Improvements. The adoption of Anaplan will revolutionise planning processes, enabling real-time resource management directly linked to HR, financial execution, and project milestones. To reinforce accountability and transparency, a dynamic dashboard will be introduced, providing organisation-wide access to KPIs covering budget performance, programme delivery, and organisational efficiency metrics.

Cross-Agency and Stakeholder Cooperation. To strengthen collaboration and operational efficiency, the ECCC will expand its shared services with EU agencies and institutions, including joint procurement to achieve economies of scale. Participation in the EUAN exchange programme will enable access to specialised expertise where needed. The ECCC will also enhance stakeholder engagement with Member States and EU institutions through advanced management tools, maintain close cooperation with the European Commission, and increase its engagement with the European Parliament and other relevant bodies.

Culture of Continuous Improvement. Finally, the ECCC will nurture a culture of innovation and wellbeing. Knowledge-sharing ecosystems will strengthen communities of practice across Operations, HR, procurement, and IT, ensuring continuous learning and the avoidance of duplicated efforts. In parallel, the organisation will leverage HR data to advance initiatives on culture, wellbeing, and diversity while building a stronger sense of community through activities involving staff and their families, and by fostering broader contributions to social responsibility.

II.2.5 Negative priorities/decrease of existing tasks

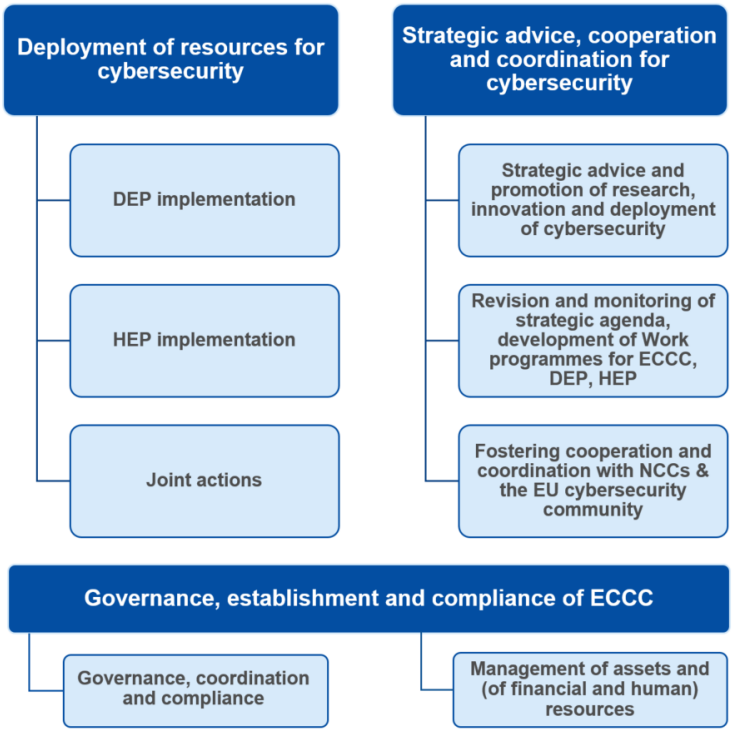
For the period covered by this SPD, the Centre will review the scope of its ongoing activities and, where relevant, reduce or discontinue those that do not contribute sufficiently to its main objectives.

SECTION III. WORK PROGRAMME 2026

III.1 EXECUTIVE SUMMARY

The overall objectives described in the multiannual outlook 2026-2028 are elaborated in the activities indicated in this section for the year 2026. In 2026 the focus will be on DEP and HEP implementation[32], 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 Cybersecurity Competence 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 2026 activities. The next sections elaborate on the context, expected activities and associated results for each of the 3 activities of the SPD.



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)*."

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

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. This includes the management of projects awarded under the DEP work programme 2023-2024, as well as the evaluation of proposals, signature of grants and management of the proposals retained for funding under the calls of the DEP work programme 2025-2027.

The Cyber Solidarity Act provides for a number of actions for the ECCC to implement. The actions related to European Cybersecurity Alert System as well as some of the actions related to the Cybersecurity Emergency Mechanism, notably preparedness actions and mutual assistance, will be implemented by the ECCC as outlined in the ECCC DEP cybersecurity WP 2025-2027[33]. The EU Action Plan on Cable Security[34] providing the possibility to launch dedicated regional integrated surveillance mechanisms focusing on sea basins. Under the Cybersecurity Emergency Mechanism, the ECCC may award grants for preparedness actions, including the coordinated preparedness testing of entities operating in sectors of high criticality (for example operators of submarine cables in line with the EU Action Plan on Cable Security) and other preparedness actions (including trainings or exercises). In addition, the ECCC may award grants for mutual assistance actions to Member States providing support to another Member State to respond to cybersecurity incidents.

The HE cybersecurity Work Programme is implemented by ECCC, according to the latest HE WP 2026-2027[35].

Important actions to be undertaken in this Activity in 2026 include the following:

Area	Expected activities	Expected results
DEP implementation	Management of projects from DEP WP 2023-2024 and WP 2025-2027. Implement the DEP calls for WP 2025-2027 (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[36] [DEP] Indicator 3.1b: Cybersecurity infrastructure and/or tools deployed: 165 infrastructure (15) and/or tools (150) deployed by 2027[37] [DEP] Indicator 3.2: Users and communities getting access to European cybersecurity facilities[38] : -150 by 2027 & 300 by 2028
HEP implementation	Possibly manage part of the 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 the DEP or the HEP	Fulfil KPIs associated with joint actions.

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

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

[33] Amendment 2 of ECCC Cybersecurity DEP WP 2025-2027, was adopted by ECCC GB decision 2025/15 and it is available from here: https://cybersecurity-centre.europa.eu/governing-board_en
[34] Joint Communication to the European Parliament and the Council- EU Action Plan on Cable Security, JOIN(2025)9 final
[35] C/2025/8493 final, from December 2025, Commission Implementation Decision on the financing of the Specific Programme implementing Horizon Europe – the Framework Programme for Research and Innovation – and the adoption of the work programme for 2026-2027
[36] [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.
[37] [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.
[38] [Method for setting the target] The target is to have at least 20 Member States using each facility.

Article 5 c) of ECCC regulation[39]. 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[40], 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, while respecting the legal requirements and budgetary allocations, in accordance with the Strategic Agenda and the multiannual work programme, priorities for the DEP and the 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. As of 2025, the ECCC prepares 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). All EU MSs and 3 associated countries have notified to the GB the entities acting as their NCCs.

Moreover, dedicated Working Groups[41] of the GB, which cooperate closely with the NCCs Network, have been established, and are listed below:

- WG 1: 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. The main objectives of this Action are to stimulate collaboration (with the Cybersecurity Competence Community, and the NCCs Network as required by ECCC regulation). 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 2023.

The Cybersecurity Competence Community should involve a large, open, and diverse group of cybersecurity stakeholders, including in particular research entities, supply/demand-side industries and the public sector, which should contribute to ECCC activities that strengthen EU strategic autonomy. Specifically, such a group provides input to the activities and work plan of the ECCC, particularly through the SAG, and it benefits from the Community-building activities of the ECCC and the Network.

[39] 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.
[40] Article 13.3(a) of the Regulation.
[41] WG have been revised during GB meeting in June 2024

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 *Coordination and Support Action*[42] from the DEP WP. The ECCC will continue to work with ENISA on surveying the cybersecurity market, including market data and analytics, databases, 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 the course of 2026 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
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 current Strategic Agenda. 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	- Adoption of the revised version of the Strategic Agenda initiated in 2025. - Report on the implementation of the current Strategic Agenda by Q4/26 - Contributions to dissemination activities regarding the Agenda and research and innovation priorities - Delivery of draft and final SPDs and WPs by statutory deadlines - Report on the implementation of the 2025-2027 DEP Work Programme by Q4/26 - 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 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.) Implement and update the indicative "service catalogue" for NCCs **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	- Well-defined and efficient coordination mechanisms are established between the ECCC and the Network of NCC. Regular workshops and meetings are organized to facilitate alignment of activities, sharing of best practices, and collaborative efforts. - ECCC supports the respective Working Groups in collaboration with ENISA. - An updated 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 Q4/26 - ECCC facilitates the functioning of SAG and supports clear organisational and technical guidelines.

III.2.3 ACTIVITY 3: Sound financial management, Governance, Human Resources and compliance

The Activity focusses on all the managerial and administrative activities required to support the operational tasks of the ECCC. In 2026, the focus will continue to 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
  - Relation with GB and ECCC stakeholders including host country; Secretariat for ECCC GB

[42] During 2023-2024 the European Commission run a project, on behalf of ECCC, to support these activities. For 2025 and 2026 the preparation work is ongoing. It included activities dedicated to the Cybersecurity Competence Community, including the "EU cybersecurity market observatory" in coordination with ENISA.

- Liaison activities with other stakeholders, (e.g. EU Agencies, International Organisations) in the remit of ECCC mandate
- Compliance and internal control
- Communication, dissemination and outreach activities

- Management of assets and (of financial and human) resources
  - Efficient and effective management of financial resources
  - Recruitment, retention and development of human resources
  - IT tools, ICT assets, security rules and other logistical aspects
  - Building and facilities management, including environmental and health and safety policy
  - Implementation of the Host Agreement
  - Monitoring, evaluations, Public Access to Documents, reporting

Actions to be undertaken in this Activity area in 2026 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 country; Secretariat for ECCC GB Liaison activities with other stakeholders, (e.g. EU Agencies, International Organisations) in the remit of ECCC mandate Compliance and internal control Implement comprehensive planning and reporting cycles integrating financial, HR, and operational data. Introduce structured risk management and performance monitoring tools to identify, assess, and mitigate emerging strategic and operational risks. Communication, dissemination and outreach activities	- 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 Q4/26 - SLAs and MoUs agreed indicating the associated efficiency gains - High level of compliance with reduced number of recommendations following audits - Revision of the communication strategy and implementation by Q4/26 - Improved strategic alignment of activities with ECCC objectives and Governing Board decisions. - Enhanced organisational accountability through integrated reporting and evidence-based decision-making. - Proactive mitigation of operational and strategic risks. - Strengthened stakeholder confidence through transparent communication and governance practices. For quantitative results, please see next table.
Management of assets and (of financial and human) resources	Efficient and effective management of financial resources Recruitment, retention and development of human resources Implementation of the Host Agreement Monitoring, evaluations, Public Access to Documents, reporting Develop competency-based HR management and a modernised careers portal to support recruitment and mobility. Map staff expertise and align roles with evolving organisational needs. Implement leadership development, mentoring, and continuous learning programmes focusing on AI literacy, project management, and data analytics. Promote well-being, inclusion, and diversity through structured engagement and HR data analysis. Develop procurement guidelines to optimise purchasing efficiency and compliance Integrate IT systems (ARES, Anaplan, Power BI, Microsoft 365) to enable end-to-end digital workflows and data coordination. Increase efforts on statutory obligation in the area of Cybersecurity Building and facilities management, including environmental and health and safety policy	- Digital workplace/IT strategy - Drafting of internal cyber security policies and rules - IT security management and business continuity arrangements - Cybersecurity awareness and exercises - Implementation of Anaplan - Streamlined workflows and reduced administrative burden through automation. - Improved data accuracy, accessibility, and interoperability across systems. - Further improvement of ECCC Facilities - Setup of satellite office in Brussels - HR policies and implementing rules in place, satisfaction of staff (survey planned for Q4/26) - Training/awareness courses on Ethics and Prevention of Harassment - Improved talent acquisition and reduced vacancy turnaround time. - Enhanced workforce agility and internal expertise for future roles. - Higher staff engagement, retention, and satisfaction. - A leadership culture fostering inclusion, professional growth, and ethical conduct - Sustainable and environmentally friendly working conditions (survey planned for Q4/26) - Procurement Acquisition Plan - Continuous coordination with Host Country - Timely reporting and timely follow up on requests, evaluations and recommendations For quantitative results, please see next table.

KPI/OKR	Target for 2026

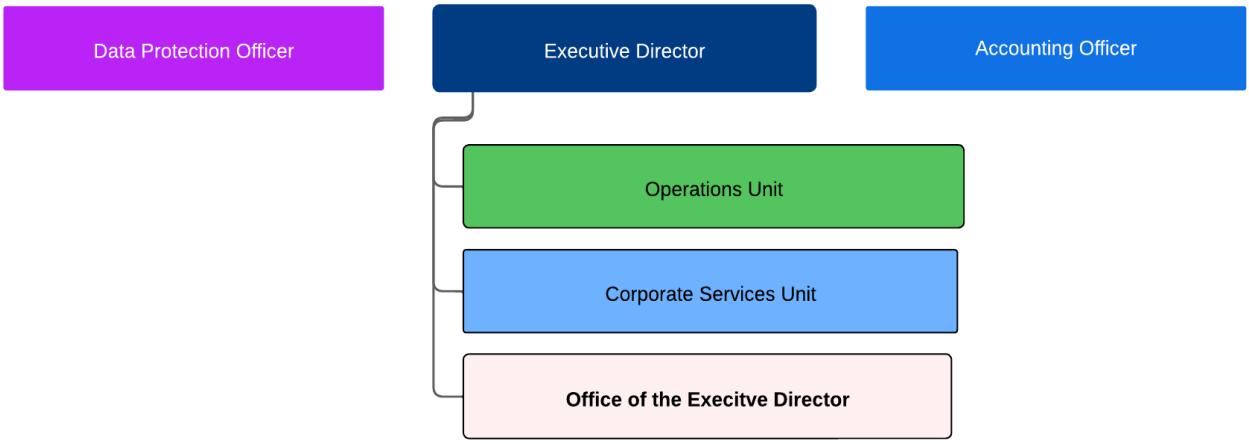
Regrettable turnover[43] rate	Below 5%
Annual occupancy rate (%)	Above 90%
Staff engagement level	Above industrial benchmark
Number of ‘critical’, ‘significant’ or ‘very important’ findings of audit bodies	Below 4
Percentage of audit recommendations implemented within deadlines	critical: 100%; very important: ≥ 85%; important: ≥ 80%
Efficient budget management - commitments implementation (%)	95% commitment rate; 95% payment rate
% of payments completed within the statutory deadlines	90% of payments on time

[43] Turnover that occurs from situations where valuable or high-performing employees leave the organization voluntarily, which the organisation would prefer to avoid.

ANNEXES

ANNEX I. ORGANISATION CHART

A high-level organisation chart has been proposed by the ED in March 2025 and is presented here below.



ANNEX II. RESOURCE ALLOCATION PER ACTIVITY 2026 – 2028

Resource allocation forecast is introduced below, with aggregated values.

No	Activity name	2026			2027			2028		
		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	170,161,120.89	4	15	189,763,754.67	4	15	189,763,754.67
2	Strategic advice, cooperation and coordination for cybersecurity	4	3	528,921.31	4	3	558,999.33	4	3	558,999.33
3	Governance, establishment and compliance of the ECCC	4	10	1,591,619.80	4	10	1,869,443.50	4	10	1,869,443.50
Total		12	28	172,281,662.00	12	28	192,192,197.49	12	28	192,192,197.49

ANNEX III. FINANCIAL RESOURCES 2026 - 2028

Budget Revenue

In accordance with the provisions of the legal framework applicable to the ECCC, for 2026 the only contributor is the EU with the budget planned for Cybersecurity activities in the DEP and in Horizon Europe Programme. 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 2026-2028 are presented in:

- table 1 –Revenue of commitment appropriations and
- table 2 –Revenue of payment appropriations.

The global revenue includes (within the indicated financial envelope) the amounts stemming from the Contribution Agreement on Horizon Europe.

Table 1 –General revenue, commitment appropriations

REVENUES	Executed 2024	Estimated 2025	2026		VAR 2026/2025	Envisaged 2027	Envisaged 2028
			Agency request	Budget forecast			
1 REVENUE FROM FEES AND CHARGES							
2 EU CONTRIBUTION	**211,267,742**	**145,449,709**	**112,838,720**		**-22%**	**117,124,426**	**117,124,426**
- Of which assigned revenues deriving from previous years' surpluses							
3 THIRD COUNTRIES CONTRIBUTION (incl. EEA/EFTA and candidate	**7,563,385**	**2,868,873**	**3,242,942**		**13%**	**3,267,771**	**3,267,771**
- Of which EEA/EFTA (excl. Switzerland)	*7,563,385*	*2,868,873*	**3,242,942**		**13%**	*3,267,771*	*3,267,771*
- Of which candidate countries							
4 OTHER CONTRIBUTIONS	96,495,097	90,550,000	56,200,000		**-38%**	71,800,000	71,800,000
5 ADMINISTRATIVE OPERATIONS			*p.m.*			*p.m.*	*p.m.*
- Of which interest generated by funds paid by the Commission by way of the EU contribution (FFR Art. 58)			*p.m.*			*p.m.*	*p.m.*
6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT			*p.m.*			*p.m.*	*p.m.*
7 CORRECTION OF BUDGETARY IMBALANCES			*p.m.*			*p.m.*	*p.m.*
TOTAL	**315,326,224**	**238,868,582**	**172,281,662**	**0.00**	**-28%**	**192,192,197**	**192,192,197**

(3) Based on EFTA percentage for DEP: 3.58% for 2024, 2.79% for 2025 and 2.64% for 2026

(4) Additional EU funding stemming from contribution agreements (FFR Art.7)

Table 2 –Total Revenue, payment appropriations

REVENUES	Executed 2024	Estimated 2025	2026		VAR 2026/2025 (%)	Envisaged 2027	Envisaged 2028
			Agency request	Budget forecast			
1 REVENUE FROM FEES AND CHARGES							
2 EU CONTRIBUTION	**188,859,092**	**186,753,417**	**158,834,439**		**-15%**	**117,124,426.00**	**117,124,426.00**
- Of which assigned revenues deriving from previous years' surpluses							
3 THIRD COUNTRIES CONTRIBUTION (incl. EEA/EFTA and candidate countries)	**6,761,155**	**5,210,420**	**4,193,229**		**-20%**	**3,267,771.49**	**3,267,771.49**
- Of which EEA/EFTA (excl. Switzerland)	*6,761,155*	*5,210,420*	**4,193,229**		**-20%**	*3,267,771.49*	*3,267,771.49*
- Of which candidate countries							
4 OTHER CONTRIBUTIONS	16,903,784	58,195,914	77,840,000.00			*p.m.*	*p.m.*
5 ADMINISTRATIVE OPERATIONS			*p.m.*			*p.m.*	*p.m.*
- Of which interest generated by funds paid by the Commission by way of the EU contribution (FFR Art. 58)			*p.m.*			*p.m.*	*p.m.*
6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT			*p.m.*			*p.m.*	*p.m.*
7 CORRECTION OF BUDGETARY IMBALANCES			*p.m.*			*p.m.*	*p.m.*
TOTAL	**212,524,031**	**250,159,751**	**240,867,668**	**0.00**	**-4%**	**120,392,197**	**120,392,197**

(3) Based on EFTA percentage for DEP: 3.58% for 2024, 2.79% for 2025 and 2.64% for 2026

(4) Additional EU funding stemming from contribution agreements (FFR Art.7)

Table 3: Additional EU funding: grant, contribution and service-level agreements, commitment appropriations

REVENUES							
REVENUES	Executed 2024	Estimated 2025	2026		VAR 2026/2025	Envisaged 2027	Envisaged 2028
			Agency request	Budget forecast			
ADDITIONAL EU FUNDING STEMMING FROM GRANTS (FFR Art.7)							
ADDITIONAL EU FUNDING STEMMING FROM CONTRIBUTION AGREEMENTS (FFR Art.7)	**96,495,097.06**	90,550,000	56,200,000		**-38%**	71,800,000	71,800,000
ADDITIONAL EU FUNDING STEMMING FROM SERVICE LEVEL AGREEMENTS (FFR Art. 43.2)							
TOTAL	**96,495,097.06**	**90,550,000.00**	**56,200,000.00**	**0.00**	**-38%**	**71,800,000.00**	**71,800,000.00**

Budget Expenditure

- table 4a – Detailed expenditure, commitment appropriations and
- table 4b – Detailed expenditure, payment appropriations.

Table 4a –Expenditure, commitment and payment appropriations

Budget line	EXPENDITURE	Budget 2024	Budget 2025	2026		VAR 2026/2025 (%)	Envisaged 2027	Envisaged 2028
				Agency request	Budget forecast			
Title 1	**Title 1 - Staff expenditure**	**1,747,000**	**3,528,500**	**4,109,566**	**0.00**	**16%**	**4,073,640**	**4,303,151**
1111	Salaries and allowances for temporary and permanent staff	950,000	1,350,000	1,752,066		30%	1,560,060	1,677,065
1121	Salaries and allowances for contractual agents	500,000	1,800,000	1,944,000		8%	2,080,080	2,236,086
1131	Seconded national experts, interim staff and trainees	100,000	100,000	120,000		20%	130,000	130,000
1141	Trainings and Recruitment	155,000	183,500	183,500		0%	183,500	140,000
1151	Social welfare and medical services	42,000	95,000	110,000		16%	120,000	120,000
Title 2	**Title 2 - Infrastructure and operating expenditure**	**901,000**	**960,000**	**1,025,000**	**0.00**	**7%**	**1,045,000**	**1,045,000**
2111	Rental of building and associated costs	290,000	60,000	70,000		17%	80,000	80,000
2121	Computer centre operations and data processing	290,000	350,000	380,000		9%	380,000	380,000
2131	Moveable property and associated costs	218,000	100,000	100,000		0%	100,000	100,000
2141	Current administrative expenditure	103,000	450,000	475,000		6%	485,000	485,000
Title 3	**Title 3 - Operational expenditure**	**312,678,224**	**234,380,082**	**167,147,096**	**0.00**	**-29%**	**187,073,557**	**186,844,047**
3111	DEP Programme	215,731,127	*142,340,082*	*109,427,096*		-23%	*113,743,557*	*113,514,047*
3121	Horizon Programme	96,495,097	90,550,000	56,200,000		-38%	71,800,000	71,800,000
3131	Evaluations and Programme tools		1,000,000	1,000,000		0%	1,000,000	1,000,000
3141	Publication, communication and trasnlation costs	**150,000**	110,000	130,000		18%	130,000	130,000
3151	Statutory, technical meetings and Studies	**222,000**	200,000	200,000		0%	200,000	200,000
3161	Missions	**80,000**	180,000	190,000		6%	200,000	200,000
	TOTAL	**315,326,224**	**238,868,582**	**172,281,662**	**0.00**	**-28%**	**192,192,197**	**192,192,197**

Table 4b – Detailed Expenditure, payment appropriations

Budget line	EXPENDITURE	Budget 2024	Budget 2025	2026		VAR 2026/2025 (%)	Envisaged 2027	Envisaged 2028
				Agency request	Budget forecast			
Title 1	**Title 1 - Staff expenditure**	**1,747,000.00**	**3,528,500.00**	**4,109,566.00**	**0.00**	**16%**	**4,073,640.00**	**4,303,150.50**
1111	Salaries and allowances for temporary and permanent staff	950,000.00	1,350,000.00	1,752,066.00		30%	1,560,060.00	1,677,064.50
1121	Salaries and allowances for contractual agents	*500,000.00*	*1,800,000.00*	*1,944,000.00*		8%	*2,080,080.00*	*2,236,086.00*
1131	Seconded national experts, interim staff and trainees	*100,000.00*	*100,000.00*	*120,000.00*		20%	*130,000.00*	*130,000.00*
1141	Trainings and Recruitment	155,000.00	183,500.00	183,500.00		0%	183,500.00	140,000.00
1151	Social welfare and medical services	42,000.00	95,000.00	110,000.00		16%	120,000.00	120,000.00
Title 2	**Title 2 - Infrastructure and operating expenditure**	**901,000.00**	**960,000.00**	**1,025,000.00**	**0.00**	**7%**	**1,045,000.00**	**1,045,000.00**
2111	Rental of building and associated costs	290,000.00	60,000.00	70,000.00		17%	80,000.00	80,000.00
2121	Computer centre operations and data processing	290,000.00	350,000.00	380,000.00		9%	380,000.00	380,000.00
2131	Moveable property and associated costs	218,000.00	100,000.00	100,000.00		0%	100,000.00	100,000.00
2141	Current administrative expenditure	103,000.00	450,000.00	475,000.00		6%	485,000.00	485,000.00
Title 3	**Title 3 - Operational expenditure**	**209,876,031.14**	**245,671,251.33**	**235,733,102.00**	**0.00**	**-4%**	**167,273,557.49**	**187,744,046.99**
3111	DEP Programme	192,520,247.25	185,985,337.33	156,373,102.00		-16%	113,743,557.49	113,514,046.99
3121	Horizon Programme	16,903,783.89	58,195,914.00	77,840,000.00		34%	52,000,000.00	72,700,000.00
3131	Evaluations and Programme tools		1,000,000.00	1,000,000.00		0%	1,000,000.00	1,000,000.00
3141	Publication, communication and trasnlation costs	150,000.00	110,000.00	130,000.00		18%	130,000.00	130,000.00
3151	Statutory, technical meetings and Studies	222,000.00	200,000.00	200,000.00		0%	200,000.00	200,000.00
3161	Missions	80,000.00	180,000.00	190,000.00		6%	200,000.00	200,000.00
	TOTAL	**212,524,031.14**	**250,159,751.33**	**240,867,668.00**	**0.00**	**-4%**	**172,392,197.49**	**193,092,197.49**

The tables above include HE contributions[44] for 2026 and 2027 which will be provided if the ECCC is entrusted by the Commission of the implementation of the cybersecurity parts under Horizon Europe pursuant to Article 5(5) of the ECCC Regulation (EU) 2021/887 to ECCC.

Table 5 - Budget outturn and cancellation of appropriations 2024

Budget outturn	2024
Revenue actually received (+)	124,955,615.00
Payments made (-)	83,308,584.00
Carry-over of appropriations (-)	18,283,430.00
Cancellation of appropriations carried over (+)	85,848.00
Adjustment for carry-over of assigned revenue appropriations from previous year (+)	
Exchange rate differences (+/-)	390.00
Adjustment for negative balance from previous year (-)	23,449,059.00
Total	

[44] C/2025/8493 final, published on 11.12.2025

Details on the use of financial resources

The list of budgetary items included in each title is presented here below.

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 (including schooling).

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	2024			2025	2026	2027	2028
ESTABLISHMENT PLAN POSTS	Authorised Budget	Actually filled as of 31/12	Occupancy rate %	Authorised staff	Envisaged staff	Envisaged staff	Envisaged staff
Administrators (AD)	10	6	60%	10	11	11	11
Assistants (AST)					1	1	1
Assistants/Secretaries (AST/SC)							
TOTAL ESTABLISHMENT PLAN POSTS	10	6	60%	10	12	12	12
EXTERNAL STAFF	FTE corresponding to the authorised budget	Executed FTE as of 31/12	Execution Rate %	Headcount as of 31/12/N-1	FTE corresponding to the authorised budget	Envisaged FTE	Envisaged FTE
Contract Agents (CA)	27	21	78%	27	27	27	27
Seconded National Experts (SNE)	1	0	0%	1	1	1	1
TOTAL EXTERNAL STAFF	28	21	75%	28	28	28	28
TOTAL STAFF	38	27	71%	38	40	40	40

**The tables include the 2 new posts received for the financial year 2026: Amendments by budget line - Consolidated document (integration of agreed amendments on DB or Council's position): Section III - Commission*[45]

[45] Please see page 45, Consolidated document, November 2025, available at: https://data.consilium.europa.eu/doc/document/ST-15487-2025-ADD-5/en/pdf

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

Not applicable.

Human Resources	2025	2026	2027	2028
	Envisaged staff	Envisaged staff	Envisaged staff	Envisaged staff
Contract Agents (CA)	0	0	0	0
Seconded National Experts (SNE)	0	0	0	0
TOTAL	**0**	**0**	**0**	**0**

C. Other Human Resources

Structural service providers[46]

	Actually in place as of 31/12/2024
Security	0
IT	0
Other (specify)	0
……	

Interim workers

	Total FTEs in year 2024
Number	1

Table 2 – Multi-annual staff policy plan 2026, 2027, 2028

Function group and grade	2024				2025		2026		2027		2028	
	Authorised Budget		Actually filled as of 31/12/2024		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												1
AD 14		1		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												2
AD 9								1		3		2
AD 8		3		3	3			3		3		2
AD 7		2		2	2			2				
AD 6												
AD 5												
AD TOTAL		10		6	10			11		11		11
AST 11												
AST 10												
AST 9												
AST 8												
AST 7												
AST 6												
AST 5								1		1		1
AST 4												
AST 3												
AST 2												
AST 1												
AST TOTAL		0		0	0			1		1		1
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		6	10			12		12		12
GRAND TOTAL		**10**		**6**	**10**			**12**		**12**		**12**

[46] (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	FTE corresponding to the authorised budget 2024	Executed FTE as of 31/12/2024	Headcount as of 31/12/2024	FTE corresponding to the authorised budget 2025	FTE corresponding to the authorised budget 2026	FTE corresponding to the authorised budget 2027	FTE corresponding to the authorised budget 2028
Function Group IV	21	16	16	21	21	21	21
Function Group III	2	2	2	2	2	2	2
Function Group II	4	3	3	4	4	4	4
Function Group I	0	0	0	0	0	0	0
TOTAL	27	21	21	27	27	27	27

Seconded National Experts

Seconded National Experts	FTE corresponding to the authorised budget 2024	Executed FTE as of 31/12/2024	Headcount as of 31/12/2024	FTE corresponding to the authorised budget 2025	FTE corresponding to the authorised budget 2026	FTE corresponding to the authorised budget 2027	FTE corresponding to the authorised budget 2028
TOTAL	1	0	0	1	1	1	1

Table recruitment forecasts 2025 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 2024 from and to the ECCC: 0.

ANNEX V. HUMAN RESOURCES QUALITATIVE

Due to limited data for the past years, part of the tables of this Annex will be filled in future SPDs.

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

Currently 63% of the workforce of the ECCC is composed of female staff with a distribution between temporary staff and contract agents as indicated in the table below. The overall gender balance across the Centre and between contract types will be taken into account in future selection processes in line with the Gender Equality Strategy 2020-2025[47].

[47] 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.

Table 1 – Data for 31/12/2024 - statutory staff

		Official		Temporary		Contract Agents		Grand Total	
		staff	%	Staff	%	Staff	%	Staff	%
Female	Administrator level			1	17%	16	76%	17	63%
	Assistant level (AST & AST/SC)			0	0%	0	0%	0	0%
	Total			1	17%	16	76%	17	63%
Male	Administrator level			5	83%	5	24%	10	37%
	Assistant level (AST & AST/SC)			0	0%	0	0%	0	0%
	Total			5	83%	5	24%	10	37%
Grand Total				6	100%	21	100%	27	100%

Table 2 – The data regarding gender evolution over 5 years of the Middle and Senior management is not presented. The Executive Director recruited as of February 2024 is the only manager in place for 2024.

D. Geographical Balance

Table 1 – Data for 31/12/2024 - 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	15	68%	5	100%	20	74%
Italian	3	14%	0	0%	3	11%
Greek	1	5%	0	0%	1	4%
Polish	1	5%	0	0%	1	4%
German	1	5%	0	0%	1	4%
Bulgarian	1	5%	0	0%	1	4%
Cypriot	0	0%	0	0%	0	0%
Total	**22**	**100%**	**5**	**100%**	**27**	**100%**

The current geographical distribution of staff shows very low diversity with a high percentage of Romanian staff and only 7 nationalities. This is partly due to the very low correction coefficient for Romania that makes salaries less competitive for similar jobs and partly due to the decentralised location of the ECCC that makes commuting more complicate for staff members with families in other countries.

In order to increase international attractiveness and staff retention, the ECCC has provided additional benefits to its staff including Schooling, VAT exemption for non-Romanian citizens, financial support for gym fees and so on. These efforts will continue in 2026 to build a more geographically balanced organisation.

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. In line with Article 2, GB/2024/5, the ECCC concludes service contracts with the concerned establishments to perform direct payments.

ANNEX VI. ENVIRONMENT MANAGEMENT

The ECCC is not registered with EMAS. The ECCC operates in a single location and shares a building with other users. The CAMPUS building in which the ECCC's premises are located is sustainable and includes features such as:

- Orientation of the heavily glazed area towards the south to obtain maximum sunlight and generate green thermal energy.
- Photovoltaic cells placed on the south facade and on the roof for generating green electricity.

- A heat recovery area at the floor level which captures solar light and heat during the day through the greenhouse effect and releases the heat throughout the building during the night.
- Automatic switching off of electric lights.
- Water-saving, automatically operated by sensors sanitary fixtures.
- The building envelope is thermally insulated.
- Indoor microclimate and lighting control and optimization systems.
- Use of building systems featuring consumption optimization and energy recovery.

The ECCC staff operate in a hybrid office/teleworking regime that helps reduce the environmental impact of commuting. The staff are encouraged to:

- use green means of transport. The CAMPUS building is equipped with charging stations for electric vehicles and bicycle racks. The ECCC premises include shower facilities for bicycle users.
- Keep document printing to a minimum.
- Behave responsibly when opening/closing windows, being aware of the need to reduce energy loss.
- Minimize the amount of waste.
- Dispose of waste in the appropriate recycling bins in the cafeterias.
- Include clauses on green public procurement in contracts.

ANNEX VII. BUILDING POLICY

The works for the Permanent Premises for the European Cybersecurity Competence Centre (ECCC) have been substantially completed in line with the defined requirements, and as of 31 March 2025, staff members have begun occupying the new facilities.

In preparation for this transition, inspections and remedial works were conducted during February and March 2025. Efforts are now focused on finalizing the remaining remedial tasks and establishing operational procedures. This includes carrying out necessary procurement activities and training staff to ensure efficient use of the premises.

The new premises offer approximately 1,775 square meters of space, designed to accommodate at least 52 individual workstations. Key features include Secured Access System, kitchen and eating facilities, lobbies, meeting rooms, Data/Server Room, quiet booths, storage areas, printing facilities, restrooms and a shower room, dedicated parking.

These facilities are expected to provide a secure and efficient working environment for ECCC staff while supporting its operational needs.

The next steps are:

- establishing procedures related to the maintenance of premises with the host.
- Perform training to staff on the use of the permanent premises.
- Initiate and finalise the procurement procedures related to the new premises
- follow up with security topics with the respective service of the EC.

ANNEX VIII. PRIVILEGES AND IMMUNITIES

The hosting agreement has been signed on 27 September 2024 and has been ratified early 2025 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

The evaluation activities of ECCC currently consists of a mixture of ex ante and ex post controls (which include following the four-eyes principle, verification of the financial circuits, operational and financial verification functions, and exceptions reporting) and a modular approach rather than the conventional ex ante / interim / ex post evaluation approach, focusing in particular on the activity level of the work programme, and relying on narrative reports linked to the specific activities.

The ECCC initiated in 2025 collects and reports on various other metrics to support efficient and effective operations at the strategic and operational level as well as process and functional levels, notably regarding its programmes implementation and its financial performance. Monitoring is carried out internally, in close coordination with the ECCC GB and in particular with the WG4 and network of NCCs for the Strategic Agenda and programmes implementation.

The upcoming evaluation for ECCC, in line with Article 38.4 of the founding regulation, that will assess the authority's performance in relation to its objectives, is intended for 2026.

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 2023[48]. 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 is in the process of completing the implementation of its Internal Control Framework, with on-going actions such as:

- Performing the risk assessment exercise for the year 2025 and providing input to the EU Agencies Network (EUAN) Peer-review risk assessment exercise 2025.
- Drafting the Business Continuity Plan (BCP) and the disaster recovery plan.
- Drafting a policy for the management of sensitive functions.
- Drafting an Internal Control Strategy.
- Updating the list of ICF indicators (Internal Control Monitoring Criteria), which constitute one of the elements on which the assurance is based.

[48] 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 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.

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[49], 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. The Action Plan is in the process of being revised, following the update of the fraud risks, as part of the general risk assessment 2025.

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

The ECCC does not receive any form of grant. Contribution Agreements, related to Horizon Europe and Digital Europe Programmes and their budgetary aspects are mentioned in Annex III.

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. Further work took place in 2023 and 2024 to support the transition to the financial autonomy. The table below presents the status of SLAs at the end of 2024.

Service-level agreement	Actual or expected date of signature	Total amount (EUR)	Duration	Counter-part	Short description
DG DIGIT	Signed	98.425,15	1 year (automatic renewal)	DIGIT	Global SLA for the provision of IT services
DG HR	signed	143.834,00	1 year (automatic renewal)	HR	SLA where DG HR provides implementation and operation of SYSPER and related services to ECCC.
PMO	Signed	12.000,00	1 year (automatic renewal)	PMO	SLA for general assistance and/or provision of applications for which the PMO is system owner
EPSO	Signed	25.000,00	1 year (automatic renewal)	EPSO	SLA providing to ECCC assistance and access to Job opportunities page, reserve lists, EPSO's planning, ex-post controls, 3rd language testing and organisation of tailor-made selections.
EUAN (EU Agencies Network)	Signed	1.000,00	Indefinite period of time	SG	SLA to mutualise the costs for the Shared Support Office
ENISA	Signed	54,604.32	1 year (automatic renewal)	ENISA	SLA for the provision of data protection officer services and accounting officer services. In addition, a MoU was signed in 2023 between ENISA and ECCC.
DG BUDG	Signed	128.220,00	1 year (automatic renewal)	DG BUDG	SLA for implementation and usage of ABAC.
e-Procurement +cloud services	Signed	30.000,00	1 year (automatic renewal)	DIGIT	Amendment to SLA for access to eProcurement tool and Cloud service
TESTA MoU	Signed	N/A	1 year (automatic renewal)	DIGIT	MoU for TESTA access/provision
CERT-EU	Signed	11.001,77	Rest of 2024, then yearly automatic renewal	DIGIT	Amendment to SLA for the use of CERT-EU
SG	Signed	19 040,00	1 year (automatic renewal)	SG	SLA for the provision of SG services (Migration to HAN)
CDT	Signed	30.102,00	1 year (automatic renewal)	CDT	Translation services and editing
RTD	Signed	N/A	1 year (automatic renewal)	RTD	eGrants (2024's amount covered by CNECT)
REA - Expert management and services	Signed	N/A	N/A	REA	No need for an SLA as we are under REA's mandate. Support of Expert management and Support services from REA

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

The ECCC signed during 2025 Memoranda of Understanding with Ukraine and with Republic of Moldova. A strategy for cooperation with third countries and/or international organisations will be prepared in the future in close coordination with the ECCC GB WG3 dedicated to international relations.

[49] 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