

DECISION No GB/2025/1

of

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

**Adopting the draft Estimate of the ECCC's Revenue and Expenditure and endorsing
the Draft 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(3) thereof;

Having regard to Recital (23) of the Regulation, according to which Commission Delegated Regulation (EU) 2019/715² 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

Provisional draft Estimate of the Agency's Revenue and Expenditure

The provisional draft Estimate of the ECCC's Revenue and Expenditure, as annexed to this decision, is hereby adopted.

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

Draft Single Programming Document 2026-2028

The draft Single Programming Document 2026-2028 including the preliminary work programme 2026, as annexed to this decision, is hereby endorsed.

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 14 January 2025,

For the European Cybersecurity Industrial,
Technology and Research Competence
Centre

(e-signed)

Pascal Steichen
Chairperson of the Governing Board

EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Draft Single Programming Document 2026-2028

Version endorsed by the ECCC Governing Board in January 2025

CONTACT

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

Email address: info@eccc.europa.eu

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

LEGAL NOTICE

This publication presents the 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 2025–2027 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.

COPYRIGHT NOTICE

© European Cybersecurity Competence Centre, 2025

This publication is licensed under CC-BY 4.0. 'Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed, provided that appropriate credit is given and any changes are indicated'.

Photos © iStock, 2025

For any use or reproduction of photos or other material that is not under the ECCC copyright, permission must be sought directly from the copyright holders.

TABLE OF CONTENT

TABLE OF CONTENT	3
FOREWORD	5
LIST OF ACRONYMS.....	6
MISSION STATEMENT.....	7
SECTION I. GENERAL CONTEXT	9
SECTION II. MULTI-ANNUAL PROGRAMMING 2026 – 2028.....	13
II.1 MULTI-ANNUAL WORK PROGRAMME	14
II.2 HUMAN AND FINANCIAL RESOURCES - OUTLOOK FOR YEARS 2026 – 2028	16
II.2.1 Overview of the past and current situation	16
II.2.2 Outlook for the years 2026 – 2028.....	16
II.2.3 Resource programming for the years 2026 – 2028.....	17
II.2.4 Strategy for achieving efficiency gains	17
II.2.5 Negative priorities/decrease of existing tasks	18
SECTION III. WORK PROGRAMME 2026	19
III.1 Executive summary	19
III.2 Activities.....	19
III.2.1. ACTIVITY 1: Deployment of resources for cybersecurity	19
III.2.2 ACTIVITY 2: Strategic advice, cooperation and coordination for cybersecurity.....	21
III.2.3 ACTIVITY 3: Governance, establishment and compliance of ECCC	23
ANNEXES	24
Annex I. ORGANISATION CHART.....	24
Annex II. RESOURCE ALLOCATION PER ACTIVITY 2026 – 2028	24
Annex III. FINANCIAL RESOURCES 2026 - 2028.....	25

Annex IV. HUMAN RESOURCES QUANTITATIVE	29
Annex V. HUMAN RESOURCES QUALITATIVE.....	31
Annex VI. ENVIRONMENT MANAGEMENT.....	32
Annex VII. BUILDING POLICY	32
Annex VIII. PRIVILEGES AND IMMUNITIES	32
Annex IX. EVALUATIONS.....	33
Annex X. STRATEGY FOR THE ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL SYSTEMS	33
Annex XI. PLAN FOR GRANT, CONTRIBUTION OR SERVICE-LEVEL AGREEMENTS.....	33
Annex XII. STRATEGY FOR COOPERATION WITH THIRD COUNTRIES AND/OR INTERNATIONAL ORGANISATIONS	34

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 the NIS 2 Directive, the amendment of Cybersecurity Act (CSA), the new Cyber Resilience Act (CRA) and the Digital Operational Resilience Act (DORA), the legislative proposals for a Cyber Solidarity Act (CSoA), the Communications on the Cybersecurity Skills Academy and on cyber defence. 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 draft multiannual planning 2026-2028 and the draft work programme for 2026. The objective is to have its final version adopted by the ECCC GB before the end of 2025. 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 DEP WP 2025-2027 and future HEP WP.

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 2024

Luca Tagliaretti

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
EU-LISA	European Union Agency for the Operational Management of Large-scale IT Systems in the Area of Freedom, Security and Justice
Europol	European Union Agency for Law Enforcement Cooperation
FTE	Full-time equivalent
GB	Governing Board (of the ECCC)
HEP	Horizon Europe Programme
ICT	Information and communication technology
ISAC	Information Sharing and Analysis Centre
IT	Information technology
JCU	Joint Cyber Unit
JU	Joint Undertaking
MoU	Memorandum of understanding
MS	Member State(s)
NCCs	National Coordination Centres
NIS	Networks and information systems
NIS CG	NIS Cooperation Group
NLO	National Liaison Officers
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)¹ is a European Union (EU) body established by Regulation (EU) 2021/887² 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)³, the Horizon Europe Program (HEP)⁴, 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 Agenda⁵ 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.

¹ https://cybersecurity-centre.europa.eu/index_en.

² Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (OJ L 202, 8.6.2021, p. 1).

³ 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).

⁴ 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).

⁵ Such Agenda is foreseen by the ECCC regulation. The ECCC Strategic Agenda, adopted by ECCC GB in March 2023 is available at: https://cybersecurity-centre.europa.eu/strategic-agenda_en

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

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

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

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

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

SECTION I. GENERAL CONTEXT

The “EU’s Cybersecurity Strategy for the Digital Decade”⁶ 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”⁷, 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 Call⁸, 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 Conclusions⁹ notably call on the EC, the High Representative of the Union for Foreign Affairs and Security Policy, and MS to carry out a risk evaluation and develop risk scenarios from a cybersecurity perspective in a situation of threat or possible attack against Member States or partner countries.

Such 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). Moreover, the political agreement on the NIS 2 Directive¹⁰ 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 has or is likely

⁶ Joint Communication to the European Parliament and the Council: The EU’s Cybersecurity Strategy for the Digital Decade, JOIN/2020/18 final.

⁷ Council conclusions on the EU’s Cybersecurity Strategy for the Digital Decade (6722/21).

⁸ ‘Nevers Call to Reinforce the EU’s Cybersecurity Capabilities’. Informal Meeting of the Telecommunications Ministers. Nevers, March 9, 2022.

⁹ <https://www.consilium.europa.eu/en/press/press-releases/2022/05/23/cyber-posture-council-approves-conclusions/>

¹⁰ Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM/2020/823 final.

to have a significant impact on services and activities¹¹, the EC to participate in crisis management coordination and situational awareness.

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

- **Revision of the NIS Directive (NIS2)**. To respond to the increased exposure of Europe to cyber threats, the EC proposed, in December 2020, a revision of the NIS Directive (NIS 2 Directive). The Directive was adopted in December 2022, and the national transposition measures shall be applied as from 18 October 2024. The new Directive raises the EU common level of ambition on cyber-security, through a wider scope, clearer rules and stronger supervision tools.
- **Cybersecurity Resilience Act (CRA)**. In September 2022, the EC presented the proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act, CRA)¹². The CRA establishes a horizontal legal framework for cybersecurity essential requirements for placing products with digital elements on the market. The CRA aims to ensure that hardware and software products are placed on the EU market with fewer vulnerabilities and that manufacturers take cybersecurity seriously throughout the whole product lifecycle. It also aims to create conditions that allow users to take cybersecurity into account when selecting and using products with digital elements. The Cyber Resilience Act entered into force in November 2024.
- **Cyber Solidarity Act**. In April 2023, the Commission adopted a proposal for a Cyber Solidarity Act, including amendments to Digital Europe Programme Regulation, designed to: (1) strengthen common coordinated Union detection capacities and common situational awareness of cyber threats and incidents; (2) reinforce preparedness and enhance response and recovery capacities to handle significant, large-scale and large-scale equivalent cybersecurity incidents; (3) enhance union resilience and contribute to effective response by reviewing and assessing significant or large-scale incidents. The Cyber Solidarity Act will complement ECCE actions to provide long-term solutions to strengthen solidarity at Union level. On 6 March 2024, the co-legislators have agreed on a political compromise text for the legislative proposal and the Cyber Solidarity Act is expected to enter into force in February 2025. The Cyber Solidarity Act provides for a number of actions for the ECCE to implement. The ECCE 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 ECCE will also be responsible under the Cybersecurity Emergency Mechanism for managing the calls for grants for the preparedness actions, including coordinated preparedness testing and other preparedness actions and managing the support within the mutual assistance action.
- **Measures for a high common level of cybersecurity for EU institutions, bodies, offices and agencies**. The EC presented a proposal for a regulation to enhance the cybersecurity and information security of the EU institutions, bodies, offices and agencies, which entered into force in December 2023. Regulation 2023/2841 puts in place a framework for governance, risk management and control across EU entities in cybersecurity, with new competences and attributions for CERT-EU and a new inter-institutional Cybersecurity Board to monitor the Regulation's implementation.
- **European Cybersecurity certification schemes**. The European Cybersecurity Certification Framework laid out in the Cybersecurity Act¹³ aims at creating market-driven European cybersecurity certification schemes and

¹¹ See please NIS 2 Directive, Article 16(2)

¹² Proposal for Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM/2022/454 final.

¹³ 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).

increasing “cybersecurity-by-design” in ICT products, services, and processes. The first European Cybersecurity Certification scheme, the Common Criteria-based European cybersecurity certification scheme (EUCC) has been adopted, and two other schemes are currently being prepared, based on preparatory work coordinated by ENISA: the European Cybersecurity Certification Scheme for Cloud Services (EUCCS) and the European 5G Certification Scheme (EU5G). In support of certification, the EU Standardisation Strategy and the current EU funding framework both include essential topics such as the development of harmonised evaluation methodologies or promoting innovations to the performance of testing ICT products, services and processes.

- **EU 5G Toolbox.** The EU 5G Toolbox¹⁴ is a comprehensive and objective risk-based approach for the security of 5G and future generations of networks. In June 2023, the NIS Cooperation Group adopted a report on the status of implementation of the EU 5G Toolbox¹⁵, which showed that a vast majority of Member States have reinforced or are in the process of reinforcing security requirements for 5G networks based on the EU Toolbox, but some of the key measures have not been fully implemented yet in all Member States. The EC also adopted a Communication on this topic at the same time¹⁶, 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 sector¹⁷ at large and identified a number of key threats that could pose significant risks for the security and resilience of the connectivity infrastructure. To mitigate these risks, a number of strategic and technical recommendations for Member States, the Commission and ENISA, are put forward.
- **EU funding in the 2021-2027 Multiannual Financial Framework.** In 2022 and 2023 funding was provided for projects on cybersecurity deployment under the DEP, and for cybersecurity research under the HEP, while further funding is foreseen under both EU programs. The respective work programmes 2023-2024, including support for cybersecurity, were adopted in 2023.
- **EU Cybersecurity Skills Academy.** In 2023 the EC adopted a non-legislative initiative outlining policy and support measures to promote cyber skills.
- **EU Cyber Defence Policy.** It was endorsed by Council Conclusions in 2023¹⁸ and it includes references to the ECCC as an essential pillar to support the scale up of European cybersecurity industry.

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

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

¹⁴ 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.

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

¹⁶ European Commission, Implementation of the 5G cybersecurity Toolbox, C(2023)4049 final, 15 June 2023.

¹⁷ 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>

¹⁸ 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>

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.

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		√	√

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

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 350 million.

The adoption of the DEP work programme 2025-2027 by the ECCC will be a major milestone during this period. 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, independently from EC services, after reaching full financial autonomy. Moreover, the EC services are expected to transfer to the ECCC the responsibility of managing existing DEP projects. 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 in the area of cybersecurity (evaluation of proposals, management of grants, etc.).

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

The ECCC will facilitate and coordinate the work of the Network of NCCs, 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

MS¹⁹. 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 Agenda²⁰ 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 activities²¹, 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.*

¹⁹ 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.

²⁰ 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.

²¹ 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**

The following activities are focused to ensure an efficient and effective management of resources, including:

- Governance, coordination and compliance
 - ED office, coordination and management of the ECCC
 - Planning and programming activities
 - 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
 - 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

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

II.2.1 Overview of the past and current situation

The ECCC Regulation entered into force on 28 June 2021. Since then, DG CONNECT has been working on the establishment of the ECCC. Preparatory actions, notably HR-related rules, were adopted in 2022 which enabled the recruitment of the majority of ECCC staff members during 2023. The EC services continued to act on behalf of the ECCC until the ECCC reached its full financial autonomy in 2024.

II.2.2 Outlook for the years 2026 – 2028

As of Q4/2024, the ECCC has taken over the full management of DEP and part of the HEP running projects in addition to providing strategic advice, coordination for cybersecurity, including the support for Working Groups and the

functioning of the NCC Network and Strategic Advisory Group. In order to fulfil its tasks, the ECCC would need to assess carefully its human and financial resources planning.

Selection and recruitment of the ECCC staff members increased significantly in 2023 and reached full capacity in 2024, including the appointment of the ED and two Heads of Units.

To improve synergies and efficiency gains, the Accounting Officer and Data Protection Officer Services are provided by ENISA since 2023 (see section below on synergies).

To be able to fulfil its tasks, the ECCC would require more staff for some of the key professional functions and support roles.

As a temporary solution, the ECCC prepared during 2024-2025 several contracts for supporting staff and the activities of ECCC engaging the stakeholders, including via *Coordination and Support Actions*. Annexes will present the outlook for such support.

II.2.3 Resource programming for the years 2026 – 2028

Financial Resources

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

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

Table 1. Appropriations for ECCC

Year	2025	2026	2027	2028
Total appropriations (EUR)	163.318.582	126.099.400	126.392.197	120.392.197

Human Resources

The Staff Regulations and Conditions of Employment of Other Servants of the EU apply to the staff of the ECCC. The first recruitments were initiated in 2022, and continued in 2023, including the selection of the ED. By 2025 all posts are expected to be filled and no new posts are foreseen for 2025-2027. 2023 recruits started to work at the temporary ECCC headquarters in Bucharest, until the final move to permanent offices (in different floors of the same building) foreseen for Q1/2025. For further info please see Annex IV.

II.2.4 Strategy for achieving efficiency gains

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

In 2023 the ECCC and ENISA signed a service-level agreement (SLA) regarding shared services for Data Protection and Accounting. Before the end of 2023 ECCC and ENISA also signed a Memorandum of Understanding (MoU), which need to be renewed on an annual basis. Please see annexes for a complete list of SLAs.

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

II.2.5 Negative priorities/decrease of existing tasks

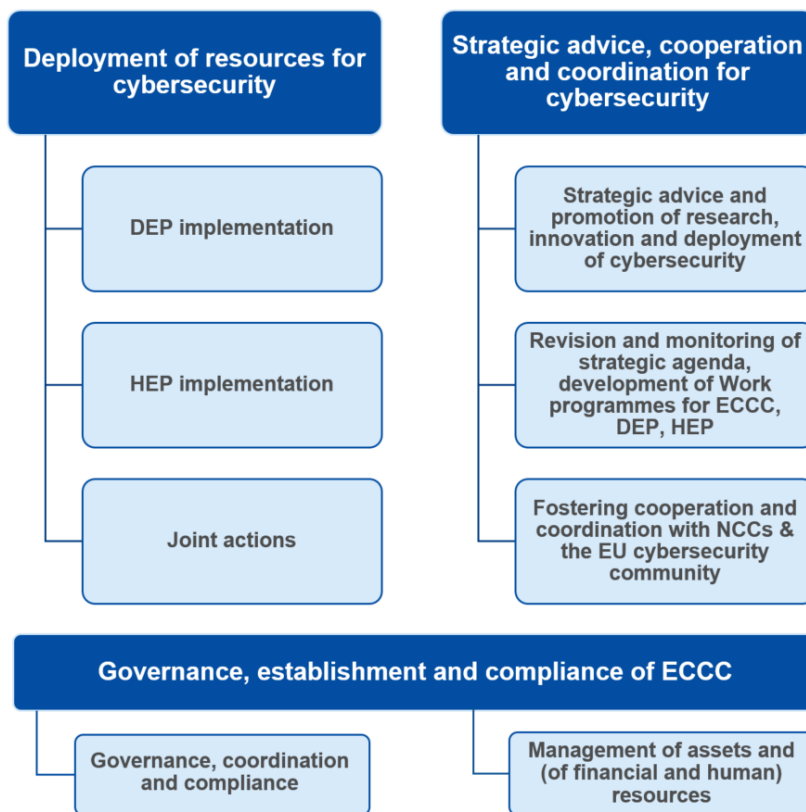
By 2025 the ECCC should be at cruising speed and tasks associated to its set-up will decrease (e.g. legal advice regarding seat agreement with host country, etc.) allowing to allocate most resources to the implementation of operational tasks. During 2026 the focus will be to assess the prioritisation done for 2025 and adjust to the context.

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 implementation²², 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

²² DEP assumes programming and execution, HEP assumes execution while Joint actions (using both DEP and HEP funding) assumes programming and execution

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)."

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. The Cyber Solidarity Act provides that the ECCC may select, based on calls for expression of interest, national Cyber Hubs and Hosting Consortia consisting of at least three national Cyber Hubs, to participate in joint procurement of tools and infrastructures. The ECCC may also award of grants for the operation of those tools and infrastructures. The ECCC is also tasked with the mapping of tools, infrastructure and services necessary and of adequate quality to establish and enhance national and Cross-Border Cyber Hubs and their availability in the Union. Under On 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 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 HEP will be gradually implemented by ECCC, as of its autonomy at the end of 2024. After DEP WP 2025-2027 will be adopted, the allocations for 2026 will be inserted here in the next version.

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

Area	Expected activities	Expected results
DEP implementation	<p>Management of projects from DEP WP 2023-2024 and WP 2025-2027.</p> <p>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</p>	<p>Launch call for proposals and follow up on it</p> <p>Fulfilment of DEP KPIs:</p> <p>[DEP] Indicator 3.1a: Cybersecurity infrastructure and/or tools jointly procured: 15 tools and/or infrastructures by 2027²³</p> <p>[DEP] Indicator 3.1b: Cybersecurity infrastructure and/or tools deployed: 165 infrastructure (15) and/or tools (150) deployed by 2027²⁴</p> <p>[DEP] Indicator 3.2: Users and communities getting access to European cybersecurity facilities²⁵ : -150 by 2027 & 300 by 2028</p>
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.

²³ [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.

²⁴ [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.

²⁵ [Method for setting the target] The target is to have at least 20 Member States using each facility.

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 Article 5 c) of ECCC regulation²⁶. 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 GB²⁷, 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. After achieving its financial autonomy, the ECCC will prepare the cybersecurity parts of the DEP work programme and contribute to the HEP work programme in accordance with the actions set out in the Strategic Agenda.

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

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

Moreover, dedicated Working Groups²⁸ 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

²⁶ 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.

²⁷ Article 13.3(a) of the Regulation.

²⁸ WG have been revised during GB meeting in June 2024

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.

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*²⁹ 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 prepared 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 set up by Q3/25. 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.

²⁹ 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.

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

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
 - 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

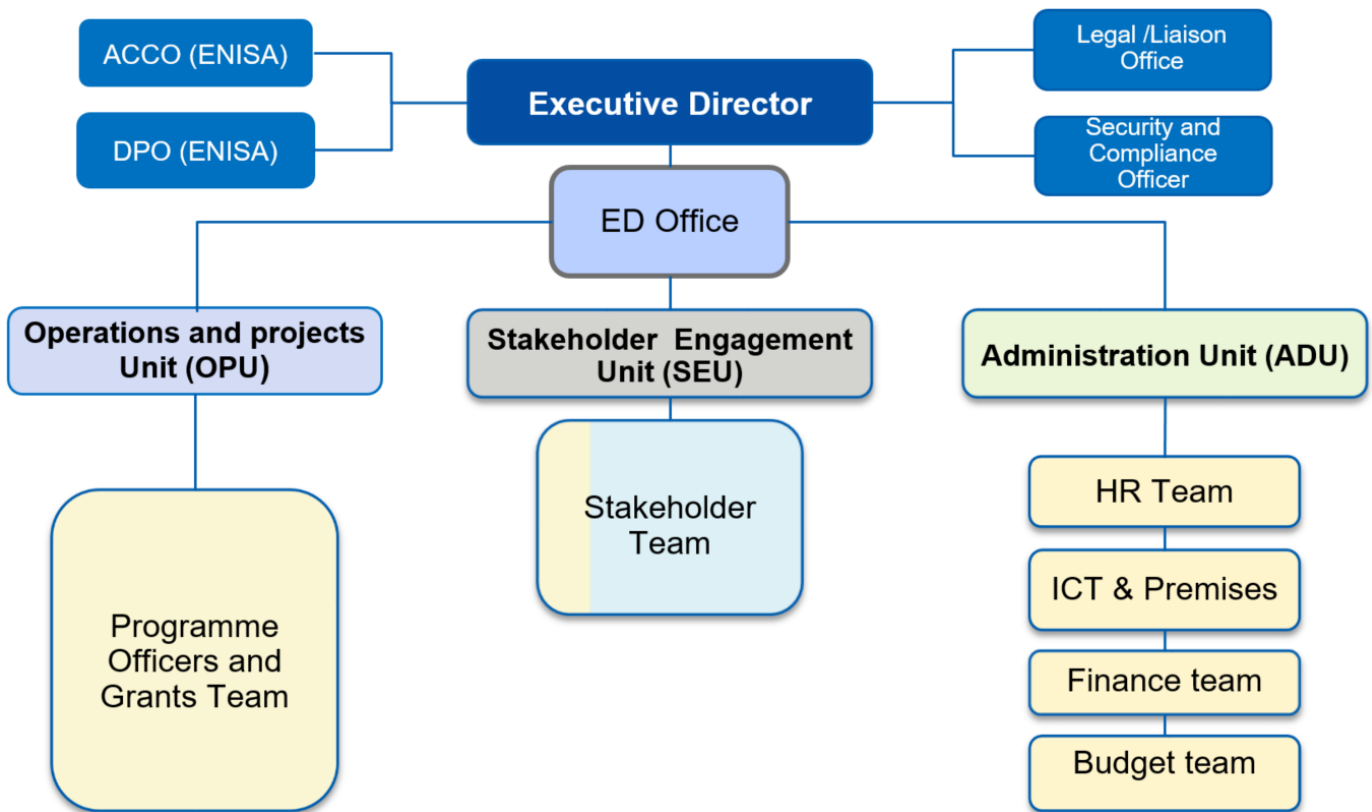
Actions to be undertaken in this Activity area in 2026 include the following:

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 Communication, dissemination and outreach activities	<ul style="list-style-type: none"> - 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
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	<ul style="list-style-type: none"> - Budget implementation in line with the ICF KPI - HR policies and implementing rules in place, satisfaction of staff (survey planned for Q1/26) - Sustainable and environmentally friendly working conditions (survey planned for Q2/26) - Continuous coordination with Host Country - Timely reporting and timely follow up on requests, evaluations and recommendations

ANNEXES

ANNEX I. ORGANISATION CHART

An organisation chart has been proposed by the ED to ECCC GB in June 2024 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	124,151,074.60	4	15	118,675,096.65	4	15	118,846,806.63
2	Strategic advice, cooperation and coordination for cybersecurity	3	3	444,925.89	3	3	471,335.33	3	3	424,201.80
3	Governance, establishment and compliance of the ECCC	3	10	1,503,400.00	3	10	1,245,765.51	3	10	1,121,188.96
Total		10	28	126,099,400.49	10	28	120,392,197.49	10	28	120,392,197.39

ANNEX III. FINANCIAL RESOURCES 2026 - 2028

Budget Revenue³⁰

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

The global revenue includes (within the indicated financial envelope) the amounts stemming from the Contribution Agreement on Horizon Europe - in tables 3a and 4a – for Revenue in terms of commitment and payment appropriations respectively.

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

Revenue	2025	2026
	Budget	Budget forecast
EU contribution	160,042,567.73	122,676,720.00
Other revenue	3,276,013.82	3,422,680.49
TOTAL REVENUES	163,318,581.55	126,099,400.49
Contributions agreement	0.00	0.00
GLOBAL REVENUES	163,318,581.55	126,099,400.49

The table above does not include HE contributions for 2025 and 2026 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 1b – Detailed table – Revenues, commitment appropriations

REVENUES	2024	2025	2026	VAR 2026/2025 (%)	Envisaged 2027	Envisaged 2028
		Total budget	Agency request			
1 REVENUE FROM FEES AND CHARGES						
2 EU CONTRIBUTION	211,267,742.00	160,042,567.73	122,676,720.00	-23%	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)	7,563,385.16	3,276,013.82	3,422,680.49	4%	3,267,771.49	3,267,771.49
- Of which EEA/EFTA (excl. Switzerland)	7,563,385.16	3,276,013.82	3,422,680.49	4%	3,267,771.49	3,267,771.49
- Of which candidate countries						
4 OTHER CONTRIBUTIONS						
5 ADMINISTRATIVE OPERATIONS						
- Of which interest generated by funds paid by the Commission by way of the EU contribution (FFR Art. 58)						
6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT						
7 CORRECTION OF BUDGETARY IMBALANCES						
TOTAL	218,831,127.16	163,318,581.55	126,099,400.49	-23%	120,392,197.49	120,392,197.49

(3) This is based on the the following EFTA percentage for DEP: 2,93 % in 2023; 3.58% for 2024 and 2.79% in 2025-2028.

³⁰ 2025 figures are based on the total financial envelope for ECCC as envisaged in the 2025 draft EU budget. EFTA percentages for DEP - 2,93 % in 2023; 3.58% for 2024 and 2.79% in 2025-2027.

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

Revenue	2025	2026
	Budget	Budget forecast
EU contribution	186,753,417.00	122,676,720.00
Other revenue	5,210,420.33	3,422,680.49
TOTAL REVENUES	191,963,837.33	126,099,400.49
Contributions agreement	0.00	0.00
GLOBAL REVENUES	191,963,837.33	126,099,400.49

The table above does not include HE contributions for 2025 and 2026 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 2b – Detailed table - Total Revenue, payment appropriations

REVENUES	2024	2025	2026	VAR 2026/2025 (%)	Envisaged 2027	Envisaged 2028
		Total budget	Agency request			
1 REVENUE FROM FEES AND CHARGES						
2 EU CONTRIBUTION	153,362,452.21	186,753,417.00	122,676,720.00	-34%	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)	5,490,375.79	5,210,420.33	3,422,680.49	-34%	3,267,771.49	3,267,771.49
- Of which EEA/EFTA (excl. Switzerland)	5,490,375.79	5,210,420.33	3,422,680.49	-34%	3,267,771.49	3,267,771.49
- Of which candidate countries						
4 OTHER CONTRIBUTIONS						
5 ADMINISTRATIVE OPERATIONS						
- Of which interest generated by funds paid by the Commission by way of the EU contribution (FFR Art. 58)						
6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT						
7 CORRECTION OF BUDGETARY IMBALANCES						
TOTAL	158,852,828.00	191,963,837.33	126,099,400.49	-34%	120,392,197.49	120,392,197.49

(3) This is based on the the following EFTA percentage for DEP: 2,93 % in 2023; 3.58% for 2024 and 2.79% in 2025-2028.

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

Revenue	2025	2026
	Budget	Budget forecast
TOTAL REVENUES	0.00	0.00

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

REVENUES	2024	2025	2026	VAR 2026/2025 (%)	Envisaged 2027	Envisaged 2028
		Agency request	Agency request			
ADDITIONAL EU FUNDING STEMMING FROM GRANTS (FFR Art.7)						
ADDITIONAL EU FUNDING STEMMING FROM CONTRIBUTION AGREEMENTS (FFR Art.7)	96,495,097.06					
ADDITIONAL EU FUNDING STEMMING FROM SERVICE LEVEL AGREEMENTS (FFR Art. 43.2)						
TOTAL	96,495,097.06	0.00	0.00		0.00	0.00

Table 4a: Overview - Additional EU funding: grant, contribution and service-level agreements, payment appropriations

Revenue	2025	2026
	Budget	Budget forecast
TOTAL REVENUES	0.00	0.00

Table 4b: Details - Additional EU funding: grant, contribution and service-level agreements, payment appropriations

REVENUES	2024	2025	2026	VAR 2026/2025 (%)	Envisaged 2027	Envisaged 2028
		Agency request	Agency request			
ADDITIONAL EU FUNDING STEMMING FROM GRANTS (FFR Art.7)						
ADDITIONAL EU FUNDING STEMMING FROM CONTRIBUTION AGREEMENTS (FFR Art.7)	16,903,783.89			#DIV/0!		
ADDITIONAL EU FUNDING STEMMING FROM SERVICE LEVEL AGREEMENTS (FFR Art. 43.2)						
TOTAL	16,903,783.89	0.00	0.00	#DIV/0!	0.00	0.00

Budget Expenditure

The ECCC total budget expenditure for the period 2026-2028 are presented in table 5a and the detailed allocation of expenditure is revealed in:

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

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

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

Expenditure	2025		2026	
	Commitment appropriations	Payment appropriations	Commitment appropriations	Payment appropriations
Title 1 - Staff expenditure	3,528,500	3,528,500	3,815,500	3,815,500
Title 2 - Infrastructure and operating expenditure	960,000	960,000	1,025,000	1,025,000
Title 3 - Operational expenditure	158,830,082	187,475,337	121,258,900	121,258,900
TOTAL Expenditure	163,318,582	191,963,837	126,099,400	126,099,400

Commitment appropriations

Table 5b – Detailed Expenditure, commitment appropriations

Budget line	EXPENDITURE	Commitment appropriations					
		Budget 2024	2025	2026	VAR 2026/2025 (%)	Envisaged 2027	Envisaged 2028
			Total budget	Agency request			
Title 1	Title 1 - Staff expenditure	1,747,000.00	3,528,500.00	3,815,500.00	8%	4,073,640.00	4,323,150.50
	1111 Salaries and allowances for temporary and permanent staff	950,000.00	1,350,000.00	1,458,000.00	8%	1,560,060.00	1,697,064.50
	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	7%	1,045,000.00	995,000.00
	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	330,000.00
	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	312,678,224.22	158,830,081.55	121,258,900.49	-24%	115,273,557.49	115,074,046.99
	3111 DEP Programme	215,731,127.16	157,340,081.55	119,738,900.49	-24%	113,743,557.49	113,544,046.99
	3121 Horizon Programme	96,495,097.06	0.00	0.00			
	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 translation 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	315,326,224.22	163,318,581.55	126,099,400.49	-0.23	120,392,197.49	120,392,197.49

Payment appropriations

Table 5c – Detailed Expenditure, payment appropriations

Budget line	EXPENDITURE	Payment appropriations					
		Budget 2024	2025	Envisaged 2026	VAR 2026/2025 (%)	Envisaged 2027	Envisaged 2028
			Total budget	Agency request			
Title 1	Title 1 - Staff expenditure	1,747,000.00	3,528,500.00	3,815,500.00	8%	4,073,640.00	4,323,150.50
1111	Salaries and allowances for temporary and permanent staff	950,000.00	1,350,000.00	1,458,000.00	8%	1,560,060.00	1,697,064.50
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	7%	1,045,000.00	995,000.00
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	330,000.00
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	173,108,611.89	187,475,337.33	121,258,900.49	-35%	115,273,557.49	115,074,046.99
3111	DEP Programme	155,752,828.00	185,985,337.33	119,738,900.49	-36%	113,743,557.49	113,544,046.99
3121	Horizon Programme	16,903,783.89	0.00	0.00	-	-	-
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 translation 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	175,756,611.89	191,963,837.33	126,099,400.49	-0.34	120,392,197.49	120,392,197.49

The tables above do not include HE contributions for 2025 and 2026 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.

Budget outturn table is not filled in for ECCC as it covers the period (2022-2023) before the financial autonomy (consistent with the approach from the previous financial year).

Details on the use of financial resources

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

TITLE 1

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

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

Details are revealed in the relevant budgetary tables.

TITLE 2

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

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

TITLE 3

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

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

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

ANNEX IV. HUMAN RESOURCES QUANTITATIVE

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

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

STAFF	2023			2024			2025			2026	2027	2028
	Authorised Budget	Filled in as of 31/12	Occupancy rate %	Authorised Budget	Filled in as of 31/12	Occupancy rate %	Authorised Budget	Filled in as of 31/12	Occupancy rate %	Authorised Budget	Authorised Budget	Authorised Budget
ESTABLISHMENT PLAN POSTS												
Administrators (AD)	10	5	50	10	6	60	10	-	-	10	10	10
Assistants (AST)												
TOTAL ESTABLISHMENT PLAN POSTS	10	5	50	10	6	60	10	-	-	10	10	10
EXTERNAL STAFF	FTE corresponding to authorised budget	Executed as of 31/12	Execution rate %	FTE corresponding to authorised budget	Executed as of 31/12	Execution rate %	FTE corresponding to authorised budget	Executed as of 31/12	Execution rate %	FTE corresponding to authorised budget	FTE corresponding to authorised budget	FTE corresponding to authorised budget
Contract Agents (CA)	27	24	89	27	21	78	27	-	-	27	27	27
Seconded National Experts (SNE)	1	0		1			1			1	1	1
TOTAL EXTERNAL STAFF	28	24	86	28	21	75	28	-	-	28	28	28
TOTAL STAFF	38	29	76	38	27	71	38	-	-	38	38	38

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 providers³¹

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

Interim workers

Total FTEs in year 2024	
Number	1

³¹ (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.

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

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

- 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	23	23	23	23
Function Group III	2	2	2	4	4	4	4
Function Group II	4	3	3	0	0	0	0
Function Group I	0	0	0	0	0	0	0
TOTAL	27	21	21	27	27	27	27

*For Contract Agents, for the years 2025-2028, while the total number is the same, the function groups were revised and updated upwards, given the current context of the ECCC, its staffing and its location.

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 3, 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

The ECCC has reached overall a gender representation with female staff representing 63% of the workforce. The distribution is not equal between temporary staff and contract agents (while it is 17% for the temporary staff it is 76% for the Contract Agents) and this will be taken into account in future selection processes in line with the Gender Equality Strategy 2020-2025³².

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

Table 2 - 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.

		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%

³² 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>.

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%

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

E. Schooling

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

ANNEX VI. ENVIRONMENT MANAGEMENT

Not applicable until permanent premises of ECCC are operational.

ANNEX VII. BUILDING POLICY

The ECCC headquarters is located in Bucharest. The ECCC opened its Temporary Premises in Bucharest located at the Politehnica Campus building in 2023. The ECCC also concluded an Administrative Agreement with the EC Representation in Bucharest, enabling ECCC staff to use the premises of EC Representation within the scope of the Administrative Agreement. The ECCC will move to its Permanent Premises by Q1/2025 located at the Campus building. The process may follow the specific provisions regarding building projects as indicated in Article 266 of the Financial Regulation applicable to the general budget of the EU.

ANNEX VIII. PRIVILEGES AND IMMUNITIES

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

The Executive Director, staff, and their family members (within the definition given by the Host Agreement) will receive a special residence card from Romania's Ministry of Foreign Affairs, granting them diplomatic privileges and

immunities. Non-Romanian nationals, including the Executive Director and their household, are accorded the same privileges as heads of diplomatic missions under the Vienna Convention, with additional benefits like car plates and residential protection upon request. If Romania grants more favourable privileges to other EU bodies in the future, the Centre and its staff will automatically receive the same treatment. Representatives of Member States participating in the Centre's work also enjoy customary privileges and immunities during their duties. Despite these privileges, the Centre, its Executive Director, and staff must respect Romanian laws and cooperate with authorities for the proper administration of justice.

ANNEX IX. EVALUATIONS

To be updated in the next versions,.

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

After the adoption of the Financial Regulation and the rules for the prevention, identification and resolution of conflict of interest (in respect of its members, bodies and staff, including the ED and the GB members, and the SARG members) by the Governing Board, the ECCC has adopted its Internal Control Framework in December 2023³³. In line with the Internal Control Framework developed by European Commission, it consists of five internal control components and 17 principles based on the COSO 2013 Internal Control-Integrated Framework.

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

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 2024³⁴, following a standalone fraud risk assessment exercise. It includes as annex the Action Plan for its implementation, which contains concrete actions for addressing the identified fraud risks.

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

The ECCC does not receive any form of grant.

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. The preparatory work started in 2021 and has resulted to concrete agreements in the course of 2022, while further work took place in 2023 and 2024 to support the transition to the financial autonomy. The table below presents the status of SLAs as of September 2024.

³³ 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

³⁴ 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

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

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

To be updated in the future SPD.