DECISION No GB/2022/24

of

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

Adopting the Single Programming Document 2023-2025 and the Statement of estimates 2023

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

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 (l), and Article 25(7) thereof;

Having regard to recital (23) of the Regulation, according to which Commission Delegated Regulation (EU) 2019/715[2] applies to the ECCC;

Having regard to Commission Communication C(2020) 2297 final, on the strengthening of the governance of Union Bodies under Article 70 of the Financial Regulation 2018/1046 and on the guidelines for the Single Programming Document and the Consolidated Annual Activity Report dated 20.04.2020;

HAS ADOPTED THE FOLLOWING DECISION:

Article 1

The Single Programming Document 2023-2025 is adopted as set out in the Annex 1 of this decision.

Article 2

The Statement of estimates for the financial year 2023 is adopted as set out in Annex 2 of this decision.

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

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

Article 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 Brussels on 22 December 2022,

For the European Cybersecurity Industrial, Technology and Research Competence Centre

(e-signed)

ANNEX 1

EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Single programming document

2023-2025

Version: ADOPTED

TABLE OF CONTENTS

FOREWORD

Our society and economy are increasingly dependent on digital technologies, while being increasingly exposed to cyber threats, which have been propelled by the Covid-19 pandemic and, more recently, by geopolitical tensions around the Russian war of aggression against Ukraine. Such greater dependence on digital technologies and rise in intensity of cyber threats call for enhanced cyber resilience, as a condition for EU stability, prosperity and autonomy while preserving an open economy.

The EU has continued developing its action on cybersecurity in various ways. These include recently adopted revision of the NIS Directive and the legislative proposal for a Cyber Resilience Act, policy initiatives such as the Communication on cyber defence, as well as funding support including three calls for proposals launched in 2022 under the Horizon Europe and Digital Europe programmes. The European Cybersecurity Competence Centre (ECCC), together with the National Coordination Centres (NCCs) are an important component of this coordinated effort to enhance cybersecurity capabilities and 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 better coordination amongst relevant stakeholders. This implies setting strategic objectives for investment, deployment, and use of cybersecurity, while pooling EU and national resources, notably the Digital Europe Program, to deliver on those objectives.

The two first Single Programming Documents (SPDs) of the ECCC, i.e. SPD 2021-2023 and SPD 2022-2024, set the foundations for the functioning of the ECCC, focusing on legal, administrative and governance aspects. SPD 2023-2025 has a greater focus on operationalisation.

In 2022 the ECCC GB became operational, holding three official meetings, electing its Chair and Vice-chair, and adopting a high number of decisions necessary for the ECCC to operate. In 2022, most NCCs were also established, while the ECCC provided NCCs with guidance and support for their activities, including opportunities to exchange amongst NCCs, EU funding for NCCs' operations and for support to third parties. NCCs should play a key role regarding the objectives of the ECCC Regulation, notably to strengthen the cyber community and collaborate with the ECCC.
In 2023, the ECCC should recruit a large part of its staff, have its long-term Executive Director (ED) appointed by the ECCC GB, move to its headquarters in Bucharest, and reach financial autonomy. In addition, the NCCs are expected to become fully operational, including in supporting potential beneficiaries of EU and national funding for cybersecurity. For all this to be achieved, EC services will continue to cooperate closely with all Member States (MS), in particular with Romania, NCCs, and the European cybersecurity agency, ENISA.

Until the ECCC reaches sufficient operational capacity and financial autonomy, European Commission (EC) services will continue acting on behalf of the ECCC, contributing with the EC's own resources. This includes preparing Digital Europe and Horizon Europe work programmes, launching and evaluating calls for proposals for both programs, and managing the projects selected for funding. The ECCC will progressively take over some of these tasks as its resources will increase over the next months.

During the period covered by this SPD (2023-2025), the ECCC and the NCCs are expected to deliver fully on their mission and objectives regarding cybersecurity investment, innovation and uptake, and thus help make the EU more cyber resilient and prosperous. The activities of the ECCC and NCCs during this period are expected to create and foster the Cybersecurity Competence Community (the 'Community').

Miguel González-Sancho, Interim Executive Director

LIST OF ACRONYMS

ABAC	Accrual-based accounting
AD	Administrator
AST	Assistant
BOA	Back Office Arrangements
CA	Contract agent
CERT-EU	Computer Emergency Response Team for the EU institutions, bodies and agencies
COVID-19	Coronavirus disease 2019
CRA	Cyber Resilience Act
CSA	Cybersecurity Act
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
DEP	Digital Europe Programme
DPO	Data Protection Officer
EC	European Commission
ECA	European Court of Auditors
ECCC	European Cybersecurity Competence Centre
ECSO	European Cyber Security Organisation
ED	Executive Director
EFTA	European Free Trade Association
EIB	European Investment Bank
ENISA	European Union Agency for Cybersecurity
EU	European Union
EUAN	EU Agencies Network
EU-LISA	European Union Agency for the Operational Management of Large-scale IT Systems in the Area of Freedom, Security and Justice
Europol	European Union Agency for Law Enforcement Cooperation
FTE	Full-time equivalent
GB	Governing Board (of the ECCC)
HE	Horizon Europe Programme
ICT	Information and communication technology
ISAC	Information Sharing and Analysis Centre
IT	Information technology
JCU	Joint Cyber Unit
JU	Joint Undertaking
MoU	Memorandum of understanding
MS	Member State(s)
NCCs	National Coordination Centres
NIS	Networks and information systems
NIS CG	NIS Cooperation Group
NLO	National Liaison Officers
SAG	Strategic Advisory Group
SC	Secretary
SLA	Service-level agreement
SMEs	Small and medium-sized enterprises
SOP	Standard Operating Procedure
SPD	Single Programming Document

TA	Temporary agent
TESTA	Trans European Services for Telematics between Administrations
TFEU	Treaty on the Functioning of the European Union

MISSION STATEMENT

The European Cybersecurity Competence Centre (ECCC) is a European Union (EU) body established by Regulation (EU) 2021/887[3] of the European Parliament and of the Council ("the Regulation"), which entered into force on 28 June 2021.

The Regulation provides the ECCC with the mandate to pursue measures in support of industrial technologies and in the domain of research and innovation. The ECCC[4] is expected to become the EU's main vehicle to pool investment in cybersecurity research, technology and industrial development, and to implement relevant projects and initiatives, together with the Network of National Coordination Centres (NCCs) and in support of the Cyber Community and relevant stakeholders. The ECCC will be in charge of managing EU financial resources dedicated to cybersecurity under Digital Europe (DEP)[5] and Horizon Europe (HE)[6] programmes, and other EU programmes where appropriate, as well as additional contributions from Member States.

The ECCC will develop and implement, with the Network of NCCs, industry and the cybersecurity technology community, a common agenda for technology development and for its wide deployment in areas of public interest and in businesses, in particular small and medium-sized enterprises (SMEs). The ECCC and the Network will contribute to Europe's technological sovereignty and open strategic autonomy through joint investment in strategic cybersecurity projects. More concretely, the ECCC and the Network of NCCs have the mission[7] 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

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

- 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 the Regulation[8], the ECCC shall have the **overall objective** of promoting research, innovation and deployment in the area of cybersecurity. Beyond its overall objective, the ECCC has the following **specific objectives**:

- Enhancing **cybersecurity capacities, capabilities, knowledge and infrastructure** for the benefit of industry, in particular SMEs, research communities, the public sector and civil society;
- Promoting **cybersecurity resilience, the uptake of cybersecurity best practices, the principle of security by design, and the certification** of the security of digital products and services, in a manner that complements the efforts of other public and private entities; and
- Contributing to a **strong European cybersecurity ecosystem** bringing together all relevant stakeholders.

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

- 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 ICT infrastructure and services** required to fulfil its tasks.

With regards to the ECCC's **tasks**[9]:

- the ECCC supported by the Network, will make strategic investment decisions and pool resources from the EU, its 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 Digital Europe and Horizon Europe programmes.
- The ECCC together with the Network will support the deployment of innovative cybersecurity solutions in the Community and beyond.

[8] Article 4 of the Regulation.
[9] Article 5 of the Regulation.

- It will also facilitate collaboration and coordination and the sharing of expertise between relevant stakeholders from the Cyber Community, in particular research and industrial communities, as well as NCCs.

SECTION I. GENERAL CONTEXT

The "*EU's Cybersecurity Strategy for the Digital Decade"*[10] outlines a strong EU vision and plan for cybersecurity. Building upon the achievements of the past months and years, 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[11] on the Joint Communication to the European Parliament and the Council entitled "*The EU's Cybersecurity Strategy for the Digital Decade*", achieving strategic autonomy while preserving an open economy is a key objective of the EU in order to self-determine its 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.

This 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 ongoing support for technical assistance and cooperation between MS for capacity-building purposes.

As highlighted in the Nevers Call[12], 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 conclusions[13] notably call on the European Commission (EC), the High Representative of the Union for Foreign Affairs and Security Policy, and MS to develop risk assessment and scenarios for an attack on a MS or partner country, which take into account relevant input and perspectives from all of the cyber communities, including civil, diplomatic and defence.

Such initiative echoes the EU's ambition for a common situational awareness and coordinated preparation and response to threats. A key priority area on which efforts are focusing is the development of shared situational awareness. This includes stronger inter-agency cooperation among ENISA, CERT-EU and Europol in assessing the threat landscape. Moreover, the political agreement

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

on the NIS Directive 2[14] provides a legal basis for the CyCLONe network of MS cyber agencies plus, in case of risks for the internal market, the EC to participate in crisis management coordination and situational awareness, is a further essential step towards solidarity and mutual assistance.

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

- **Revision of the NIS Directive (NIS2).** To respond to the increased exposure of Europe to cyber threats, the EC proposed, in December 2020, a revised NIS Directive (NIS 2 Directive), for which the co-legislators reached a political agreement in May 2022. The new Directive will raise the EU common level of ambition on cyber-security, through a wider scope, clearer rules and stronger supervision tools.

- **Cybersecurity Resilience Act (CRA).** In September 2022, the EC adopted the proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act, CRA)[15]. The CRA establishes a uniform legal framework for 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 manufacturers take cybersecurity seriously throughout the whole product lifecycle. It also aims to create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements.

- **Cybersecurity – uniform rules for EU institutions, bodies and agencies.** The EC has presented a proposal to enhance the cybersecurity and information security of the EU institutions, bodies and agencies, which are now under consideration by the legislators.

- **European Cybersecurity certification schemes**. The European Cybersecurity Certification Framework laid out in the Cybersecurity Act[16] aims at creating market-driven and least fragmented EU certification schemes and increasing trust in "cybersecurity-by-design" ICT products, services, and processes. Three schemes are currently being prepared, based on preparatory work coordinated by ENISA: the Common Criteria-based European cybersecurity certification scheme (EUCC), the European Cybersecurity Certification Scheme for Cloud Services (EUCS) and the European 5G Certification Scheme (EU5G). In support of certification, the EU Standardisation Strategy and the current EU funding framework both include essential topics such as the development of harmonised evaluation methodologies or innovations to the performance of testing ICT products, services and processes.

[14] 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.
[15] Proposal for Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM/2022/454 final.
[16] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

- **EU 5G Toolbox.** The EU 5G Toolbox[17], which is currently being implemented at EU and national level, is a comprehensive and objective risk-based approach for the security of 5G and future generations of networks. While work is still ongoing in some MS, a vast majority of MS have already reinforced or are in the process of reinforcing security requirements for 5G networks based on the EU Toolbox, including putting in place frameworks for imposing appropriate restrictions on 5G suppliers considered to be high-risk. In addition, MS, with the support of the EC and ENISA, assessed the cybersecurity of Open Radio Access Networks ('Open RAN')[18], which will in the coming years provide an alternative way of deploying the radio access part of 5G networks based on open interfaces.

- **EU funding in the 2021-2027 Multiannual Financial Framework.** Funding is foreseen for cybersecurity deployment under the Digital Europe programme, and for cybersecurity research under the Horizon Europe programme.

- **Cooperation on cyber detection, analysis and sharing.** In the face of the growing number and impact of cybersecurity incidents, the EU Cybersecurity Strategy stresses the urgent need to improve our collective detection capacities. A lot of potential for improving detection of cyber threats and incidents can come through creating, reinforcing and connecting relevant entities such as Security Operation Centres (SOCs), Computer Emergency Response Teams (CERTs), Computer Security Incident Response Teams (CSIRTs), Information Sharing and Analysis Centres (ISACs), as well as sharing of cyber threat intelligence across the EU. The ECCC will play a central role in capacity building (e.g., through grants under the Digital Programme), and by taking on a central role in joint procurement with MS, with the aim to set up several cross-border platforms for pooling data on cyber threats between several MS.

- **EU Cyber Solidarity Initiative.** The Commission will prepare an EU Cyber Solidarity Initiative, including a possible Act to make legislative changes to DEP: (1) to strengthen common EU detection, situational awareness and response capabilities. (2) to gradually build an EU-level cyber reserve with services from trusted private providers. (3) to support testing of critical entities for potential vulnerabilities based on EU risk assessments. This support mechanism will complement ECCC actions to provide long-term solutions to strengthen EU cyber security.

Within this broader framework of EU policy priorities in cybersecurity, 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 HE and DEP. For instance, the ECCC will support the development of capabilities for early threat detection and sharing of cyber threat intelligence (CTI), reinforcing and linking the capabilities of SOCs and other relevant entities in the

[17] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Secure 5G deployment in the EU - Implementing the EU toolbox, COM(2020) 50 final.

[18] NIS Cooperation Group, Report on the cybersecurity of Open RAN, 11 May 2022, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-open-radio-access-networks.

EU. The ECCC will also enable further alignment with actions funded under the Recovery and Resilience Facility and the European Structural and Investment Funds, whose implementation to a large extent lies in the hands of MS and regional authorities.

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

The ECCC, the Network and the Community are intended to benefit from the experience and the broad representation of relevant stakeholders built through the public-private partnership on cybersecurity between the EC and the European Cyber Security Organisation (ECSO) as well as from the lessons learnt from relevant projects[19] under Horizon 2020.

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

In general, the multiannual work programme shall be reflecting the EU's policy priorities and the Agenda[20], while containing common, industrial, technology and research priorities which are based on the needs identified by MS in cooperation with the Community and which require the focus of EU financial support, including key technologies and domains for developing the EU's own capabilities in cybersecurity (*Article 13 of the Regulation*).

In 2022 the foundation was laid for the first Agenda of the ECCC which will be adopted in 2023 and then will guide future SPDs. The SPD 2023-2025 should be adopted as soon as possible, since its adoption is a prerequisite for the implementation of the ECCC 2023 budget, and the swift preparation of the next SPD for 2024-2026. The SPD 2023-2025 will be the last one of the ECCC's initial establishment phase, while from next year, the standard timeline of the annual SPD exercise will be followed.

[19] CONCORDIA, ECHO, SPARTA and CyberSec4Europe.

[20] The Agenda, as defined in Article 2 point (8) of the Regulation, means "*a comprehensive and sustainable cybersecurity industrial, technology and research strategy which sets out strategic recommendations for the development and growth of the European cybersecurity industrial, technological and research sector and strategic priorities for the Competence Centre's activities and is not binding with respect to decisions to be taken on the annual work programmes*".

SECTION II. MULTI-ANNUAL PROGRAMMING 2023 – 2025

1. MULTI-ANNUAL WORK PROGRAMME

The Activities for the Multiannual Work Programme 2023-2025 of the ECCC fall under the following four (4) main objectives:

- **Objective #1:** Achieve full financial autonomy

Activities covered under this objective were predominant in the first two SPDs of the ECCC (2021-2023 and 2022-2024) and remain so for this Work Programme, given that the ECCC is still in its establishment and initial operation phase. Such activities are expected to decrease by the time the ECCC reaches its financial autonomy, which is expected over the course of 2023. Until then, the functions and duties of the ECCC are ensured by the EC services, who act on behalf of the ECCC for the establishment and initial operation[21].

Key tasks and related decisions cover notably the following areas:

- Governance and management of the ECCC:
  - Selection of the ED and take-up of duties
  - Launch of the EU Cybersecurity Competence Community
  - Organise the selection and appointment of members of the Strategic Advisory Group (SAG)
  - Programming documents
  - Development of a public communication and dissemination policy
  - Selection and appointment of the Accounting Officer
  - Adoption of decisions, rules and procedures for the further operationalisation of the ECCC
- Infrastructure:
  - Premises: fitting out and delivery of hosting premises (permanent and temporary), conclusion of respective rental agreements with the Romanian Government
  - Further support from the host MS, including conclusion of the Host Agreement with the Romanian Government
  - Transfer to ECCC's headquarters to Bucharest
  - Logistics
- Staff:
  - Selection and recruitment of staff members
  - Management of staff

[21] Article 46 of the Regulation.

- Integration and training
- Development of necessary functions and developing capacities
- Growth and adaptation of internal structure
- Support from the host MS on the integration of first staff members in Bucharest

• **Objective #2:** Implement DEP and, where relevant, HE

For this Work Programme, the main funding sources foreseen will come from DEP. The approximate estimated budget for the Cybersecurity part of DEP during the 3-year period 2023-25 is EUR 419,78 million.

The adoption by the EC of the DEP work programme 2023-2024 will be a major milestone during this period. Key tasks will be the evaluation of the calls for proposals, the signature of grants and the management of the projects receiving funding. Until the ECCC reaches full financial autonomy, the EC services will carry out the aforementioned tasks and will act on behalf of the ECCC. ECCC staff members will assist with the implementation of the funding programmes and will gradually take up responsibilities according to the administrative capacity of the ECCC.

The adoption of the ECCC's Agenda, aligned with the Digital Europe programme, will shape the strategic direction of the ECCC.

Participation of the ECCC in Horizon Europe is not foreseen in the short term. Should the ECCC decide differently, this will be reflected in an amendment of the Horizon Europe Work Programme. Provided that the ECCC has achieved financial autonomy, the ECCC may decide on the work programme for the Horizon Europe to the extent that actions are co-financed by MS. In addition, the EC may decide to delegate to the ECCC the implementation (proposal evaluation, management of grants) of further Horizon Europe actions in the area of cybersecurity.

• **Objective #3:** Develop, implement and monitor the Agenda of the ECCC, the multiannual work programme and the annual work programme

The Agenda of the ECCC, which is to be adopted by the Governing Board (GB), will be a comprehensive and sustainable cybersecurity industrial, technology and research strategy which sets out recommendations for the development and growth of European cybersecurity capabilities and priorities for the ECCC's activities[22]. A dedicated Working Group of the GB has been working on drafting the Agenda of the ECCC over the course of 2022, with the aim of having it finalised and adopted by the GB early 2023.

Once adopted, the Agenda should guide the drafting of the next annual and multiannual work programmes of the ECCC.

After financial autonomy will be achieved, the annual work programme of the ECCC will define, in accordance with the Agenda and the multiannual work programme, the cyber priorities for the Digital Europe Programme and, to the extent that they are co-financed by the MS, also the priorities for the

[22] Article 2 point (8) of the Regulation.

Horizon Europe programme. These work programmes will include, where relevant, joint actions between the ECCC and MS.

When drafting the Agenda, 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 SAG, when they will be in place, and from ENISA.

- **Objective #4:** Build and coordinate the Network of National Coordination Centres and the Cybersecurity Competence Community

The ECCC should facilitate and coordinate the work of the Network of NCCs. The Network should be composed of one NCC from each MS[23]. The modalities for interactions within the Network shall be further specified. With the exception of two MS, all MS had already notified to the GB the entities acting as their NCCs by September 2022. Over the course of 2022, seven dedicated Working Groups of the GB were established with the aim of providing support to the function of the NCCs Network:

- WG1-Community membership and registration.
- WG2-NCCs Reference Manual (working title, pending a final title).
- WG3-NCCs Network functioning.
- WG4-Strategic Agenda.
- WG5-Cyber Skills.
- WG6-Collaboration with Ukraine.
- WG7-Security Operation Centres (SOCs).

The ECCC should stimulate and support the long-term strategic cooperation and coordination of the activities of the Community. The latter would gather a large, open, interdisciplinary and diverse group of European stakeholders involved in cybersecurity technology. The Community should include academic and research entities, industries and the public sector. It is open to other EU and MS bodies (including ENISA and others) and relevant stakeholders (e.g. ECSO). Relevant activities should increase the visibility of EU cybersecurity expertise, products and services. According to the Regulation, the assessment is made by the NCCs, and the NCCs should cooperate through the Network and align the procedures they follow for assessing entities. Over the course of 2022, the GB adopted a decision on guidelines for assessing and registering entities as members of the Community[24] to provide support to NCCs and ensure a minimum level of alignment.

After its appointment by the GB, the SAG shall regularly advise the ECCC in respect of the performance of the ECCC's activities and shall ensure communication with the Community and other

[23] 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.

[24] Decision No GB/2022/7 of the ECCC Governing Board on the Community membership and registration guidelines.

relevant stakeholders. The Community, in particular through the SAG, should provide input to the activities of the ECCC, to the multiannual work programme and to the annual work programme.

In the context of the NCCs and the Community, it will be important to increase the visibility for EU cybersecurity expertise, products and services. Based on the efforts of the NCCs, the four pilot projects, local/regional efforts in MS, and the "Cybersecurity Atlas"[25] platform, the ECCC will seek to bring together resources and knowledge on the cybersecurity market. This may include interconnecting relevant tools and platforms. The NCCs will have a primary role in providing, facilitating, and collecting relevant information. This would enable the creation of market intelligence and insights, as well as provide an EU-wide overview of the cybersecurity ecosystem.

The Cybersecurity Atlas will continue its pivotal role as a knowledge management platform to map, categorise and stimulate collaboration between European cybersecurity experts, and it will also be extended to present NCC activities and information at European level.

Operational support to the mission of the NCCs, and their functioning as a network, and to the European Cybersecurity Competence Community, including the organization of industrial matchmaking and partnering events, will come online in 2023 through a dedicated service contract procured through the DEP Call 'Cybersecurity Community Support' (CNECT/2022/OP/0033).

The EC, the European Investment Bank (EIB) and the European Investment Fund are currently looking at options to create additional private investment opportunities in Cybersecurity through the InvestEU instrument, based on a market study recently performed by the EIB. The ECCC will look for synergies with the EIB whenever relevant.

2. HUMAN AND FINANCIAL RESOURCES - OUTLOOK FOR YEARS 2023 – 2025

2.1 OVERVIEW OF THE PAST AND CURRENT SITUATION

The Regulation entered into force on 28 June 2021. Since then, DG CONNECT of the EC has been working on the establishment of the ECCC. In the short period during which the ECCC existed in 2021, preparatory actions were taken regarding future recruitment of staff, notably adoption of HR-related legal framework, while no staff members were yet recruited during 2021[26]. The ECCC 2021 budget was adopted towards the end of 2021 (Decision No GB/2021/8). During 2022, further preparatory actions, notably HR-related rules, were adopted which enabled the recruitment of the first staff members of the ECCC. The ECCC 2022 budget was adopted during spring 2022 (Decision No GB/2022/6). The EC services continue acting on behalf of the ECCC until the ECCC reaches full financial autonomy.

[25] European Cybersecurity Atlas | Cybersecurity Atlas (europa.eu).
[26] For more details on staff recruitment, see points IV and V under "Annexes".

2.2 OUTLOOK FOR THE YEARS 2023 – 2025

This work programme aims to provide the ECCC activities with the necessary legal and budgetary resources during its establishment and initial operation phase. Selection and recruitment of the initial staff members of the ECCC which started in 2022 will continue during 2023 and the following years, in order for the ECCC to become operational. The long term ED, as well as the Accounting Officer of the ECCC, will be taking over their duties in the course of 2023. Moreover, the premises of the ECCC selected in 2022 will be ready for use during 2023. These are the most important actions requiring legal and budgetary resources for the ECCC to start its basic activities and pave the way towards its full autonomy in 2023.

The adoption of this Work Programme will enable the ECCC to:

- Continue the recruitment of staff with the targets indicated in section 2.3.2.
- Proceed with the fitting-out and delivery of the premises that will host the headquarters of the ECCC in Bucharest, based on relevant decisions by the GB and agreements with the Romanian government.
- Gradually take over the implementation of the Digital Europe Programme (and Horizon Europe programme, if applicable), including the evaluation of the calls for proposals, the signature of grants and the management of the projects receiving funding.
- Adopt, implement and monitor the Agenda of the ECCC, which shall guide the drafting of the next annual and multi-annual work programmes of the ECCC.
- Fulfil its mandate as described in the Mission Statement by performing the activities described in this Work Programme.
- Support the mission of the NCCs and their functioning as a Network of NCCs, as well as the Cybersecurity Competence Community.

2.3 RESOURCE PROGRAMMING FOR THE YEARS 2023 – 2025

2.3.1 Financial Resources

As defined in the Regulation, the ECCC shall in principle be funded by the EU, while joint actions shall be funded by the EU and by voluntary contributions from MS.

Generally, 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 Horizon Europe 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 2023, all budget projected below will come from DEP appropriations. The further evolution of the planned total EU contribution for 2024–2025, as well as for the full period of the new multiannual financial framework 2021–2027, is not yet available.

Table 1

	2023	2024	2025
Total appropriations for ECCC *(EUR)*	184 304 855	114 450 176	121 029 703[27]

2.3.2 Human Resources

The seat of the ECCC will be in Bucharest. Until the headquarters building for the ECCC is ready for use, transitory measures for the staff of the ECCC will be put in place.

The first staff recruitments took place in 2022 and further recruitments will be made in the course of 2023, including the selection of the ED.

In accordance with Article 30(3) of the Regulation, the GB adopted a decision, in the beginning of 2022, delegating the relevant appointing authority powers to the interim ED and the ED. The Staff Regulations and Conditions of Employment apply to the staff of the ECCC.

For the establishment and initial operation of the ECCC, the EC has designated an interim ED until the ED takes up his or her duties following his or her appointment by the GB (Article 46(2) of the Regulation).

2.4 STRATEGY FOR ACHIEVING EFFICIENCY GAINS

The ECCC is committed to continuously implement measures to obtain efficiency gains in all activities. A detailed strategy will be developed when the ECCC is fully operational. During the setting-up and initial operation phases, the EC services are entrusted with the tasks and duties of the ECCC. For example, the EC services will ensure the functioning of the ECCC during this

[27] This is based on the 2023 percentage for EFTA: 2,93 % for DEP.

phase with regard to payments and practical arrangements related to budget execution, until the ECCC reaches full autonomy, including having in place the required IT tools.

Whenever possible, the ECCC will seek synergies and the most efficient ways of action. On July 2022, the ECCC became an ad hoc member of the EU Agencies Network (EUAN), which gives access to a Network of agencies, JUs (Joint Undertakings) and other EU bodies, and the opportunity to exchange knowledge and best practices on horizontal issues for EU bodies.

Moreover, since the beginning of the ECCC's establishment phase in 2021, the EC, acting on behalf of the ECCC, has been exploring synergies with other agencies, JUs and EU bodies. More concrete actions are expected over the course of 2023, in particular regarding cooperation with ENISA, including the signature of a service-level agreement (SLA) between the ECCC and ENISA regarding shared services (namely Data Protection Officer and Accounting Officer services).

In parallel, the EC, acting on behalf of the ECCC, is following the developments around the Back Office Arrangements for Joint Undertakings (BOA/JUs)[28] and might propose that the ECCC should be more actively involved and benefit from such arrangements at a later stage.

The following table summarises the referred activities:

Objectives	Expected results
Premises/Infrastructure	Fitting out and handover of the premises offered by the host state, in line with all necessary requirements
	Conclusion of an agreement regarding the premises with the Romanian Government
	Launching of negotiations and possible signature of the rental agreement with the Romanian Government regarding the permanent premises
	Launching the implementation of the fitting-out of the permanent building in line with all the necessary requirements
	Submission of the relevant building file to European Parliament and Council, as necessary
	Finalisation of negotiations and signature of the Host Agreement with the Romanian Government
	Setting-up the necessary IT infrastructure for the ECCC operations

[28] According to the Single Basic Act (article 13), by 30.11.2022, Joint Undertakings shall operate Back Office Arrangements (setting out common corporate lines) by concluding service level agreements. BoA should cover areas like human resource support, legal support, accounting, communication, et al.

Governance and management (structure, legal & procedural framework)	Selection, appointment and take-up of duties of the ECCC ED
	Adoption of programming documents
	Accelerate the registration of members of the EU Cybersecurity Competence Community
	Set-up of the Strategic Advisory Group (appointment of members, rules of procedure) after establishment of EU Cybersecurity Competence Community
	Development of a public communication and dissemination policy
	Appointment of the Accounting Officer
	Financial rules (tbc)
	Adoption of the Internal control framework rules
	Adoption of the Anti-fraud and anti-corruption strategy and protection measures for persons reporting on breaches of EU law
	Rules for the prevention, identification and resolution of conflicts of interest in respect of its members, bodies and staff, including the ED and the GB members, and SAG members (tbc)
	Adoption of the ECCC's Security rules
Staff	Rules on the secondment of SNEs and the use of trainees
	ECCC's financial autonomy validation
	Approval of working arrangements between the ECCC and EU institutions, bodies, offices and agencies (e.g. ENISA, EEAS, JRC, REA, HADEA, Europol, EDA etc.) and international organisations, where relevant
	Adoption of further HR-related legal framework (e.g. implementing rules to the Staff Regulations and to the Conditions of Employment of Other Servants of the EU-CEOS)
	Selection and recruitment of staff members of the ECCC
	Management and integration of initial staff, including necessary trainings

SECTION III. WORK PROGRAMME 2023

1. EXECUTIVE SUMMARY

The overall objectives described for the multiannual outlook 2023-2025 are elaborated in the activities indicated in this section. The priority for 2023 are a substantial recruitment of staff members (over 20), completing the fulfilment of administrative and operational capabilities of the ECCC, the fitting-out and delivery of headquarters premises. Other activities will include the adoption of the Agenda of the ECCC, the full roll-out and operation of the Network of NCCs and of the Cybersecurity Competence Community and support to the implementation of Digital Europe Programme.

2. ACTIVITIES:

2.1 ACTIVITY DOMAIN #1: LEGAL AND OPERATIONAL ACTIVITIES FOR THE SETUP OF THE ECCC

The activities described under this chapter are related to Objective #1 of the Multiannual Work Programme: "*Achieve full financial autonomy*".

The completion of the setting-up of the ECCC, which started in the second half of 2021, is one of the main challenges for 2023. Once the establishment phase is over, the ECCC will become fully autonomous and will be able to focus on its operational tasks, benefitting from the governance structures, rules, procedures and infrastructure in place.

The administrative budget of the ECCC will cover the expenditures required to accomplish the activities described in this section during the establishment and initial operation period of the ECCC. These may include, but are not limited to: reimbursement of travel expenses of GB members, advisory services for establishment of headquarters in hosting country, expenses for contracting staff as well as integrating and training that staff, salaries, costs related to the conditioning and refurbishment of premises, costs related to procurement and integration of ICT systems.

See also chapter 2.4 (under Section II) on strategy for efficiency gains.

2.2 ACTIVITY DOMAIN #2: IMPLEMENTATION OF DIGITAL EUROPE AND HORIZON EUROPE PROGRAMME

The actions under Specific Objective 3 (Cybersecurity and Trust) of the DEP will be implemented primarily through the ECCC and the Network of NCCs.

Along 2023 and until the ECCC reaches financial autonomy, the EC services will act on behalf of the ECCC. This includes the management of projects awarded under the first call of the DEP work programme 2021-2022, the evaluation of proposals under the second call and the signature of grants and the management of the proposals retained for funding under that call, and the adoption of the DEP work programme for 2023-2024 (by EC decision and comitology). Most of those tasks will be gradually transferred to the ECCC according to its administrative capacity.

Important actions to be undertaken in this activity area in 2023 include the following:

Objectives	Expected results
Programme implementation	EC implementing DEP calls on behalf of the ECCC for WP 2023-2024 (take financing decisions, launch calls, organise evaluations, conclude grant agreements)
	Annotated Model grant agreement adoption[29]
	Where necessary, development of approach/ methodology to calculate MS in-kind contribution[30]
	Identify possible Joint Actions to be supported by contributions from some MS and by EU budget from DEP or HE[31]

The following tables summarise the WP 2021-2022 calls and topics:

	1. First call 2021-2022	
	Topic	Indicative budget (EUR million)
DIGITAL-2022-CYBER-02-NAT-COORDINATION	*Deploying The Network of National Coordination Centres with Member States*	33 (out of total 55)
DIGITAL-2022-CYBER-02-SUPPORTHEALTH	*Support to Cybersecurity in the Health Sector*	10

[29] Started in 2022.
[30] Started in 2022.
[31] Started in 2022.

	2. Second call 2021-2022	
	Topic	Indicative budget (EUR million)
DIGITAL-ECCC-2022-CYBER-03-CYBER-RESILIENCE	*Cybersecurity Resilience, Coordination and Cybersecurity Ranges*	15
DIGITAL-ECCC-2022-CYBER-03-UPTAKE-CYBERSOLUTIONS	*Uptake of Innovative Cybersecurity Solutions*	32
DIGITAL-ECCC-2022-CYBER-03-SOC	*Capacity building of Security Operation Centres (SOCs)*	72,5
DIGITAL-ECCC-2022-CYBER-03-SEC-5G-INFRASTRUCTURE	*Securing 5G Strategic Digital Infrastructures and Technologies*	10
DIGITAL-ECCC-2022-CYBER-03-NAT-COORDINATION	*Deploying the Network of National Coordination Centres with Member States*	22 (total 55)
DIGITAL-ECCC-2022-CYBER-03-NIS-DIRECTIVE	*Supporting the NIS Directive*[32] *Implementation and National Cybersecurity Strategies*	20
DIGITAL-ECCC-2022-CYBER-03-TEST-CERT-CAPABILTIES	*Testing and Certification Capabilities*	5
Procurement	*Support for Community Building,*	3

2.3 ACTIVITY DOMAIN #3: ADOPTION OF THE AGENDA, THE MULTIANNUAL WORK PROGRAMME AND THE ANNUAL WORK PROGRAMME

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 strategic recommendations for the development and growth of the European cybersecurity industrial, technological and research sector, and strategic priorities for the ECCC's activities, and is not binding with respect to decisions to be taken on the annual work programmes.

The Agenda, as adopted by the GB [33], should be reflected in the drafting of the annual work programme and the multiannual work programme. More specifically, given that the Agenda is about setting out strategic recommendations and priorities for the ECCC's activities, and shall also be reflected in the multiannual work programme, the EC provided input to the ECCC's Agenda in the course of 2022, in close cooperation with the GB and the Network. A dedicated Working Group of the GB has been working on drafting the Agenda of the ECCC over the course of 2022, with the aim of having it finalised and adopted by the GB early in 2023.

[32] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).
[33] Article 13.3(a) of the Regulation.

Once adopted, the Agenda should guide the drafting of the next annual and multiannual work programmes of the ECCC.

After financial autonomy has been achieved, the annual work programme of the ECCC will define, in accordance with the Agenda and the multiannual work programme, the priorities for the DEP and, to the extent that they are co-financed by the MS, also the priorities for the Horizon Europe programme. These work programmes will include, where relevant, joint actions between the ECCC and MS.

Important actions to be undertaken in this activity area during the period which completion is expected over the course of 2023 include the following:

Objective	Expected results
Agenda	Adoption of the agenda, following consultation with all relevant actors (EC, NCCs, Community, ENISA, SAG)
	Once adopted, monitoring the implementation of the Agenda
Multiannual work programme & Annual work programme	Development, adoption and monitoring of the multiannual work programme and the annual work programme

2.4 ACTIVITY DOMAIN #4: ACTIVITIES RELATED TO THE NETWORK OF NATIONAL COORDINATION CENTRES AND THE CYBERSECURITY COMPETENCE COMMUNITY

The Network of NCCs is composed of all NCCs that will be notified to the GB by the MS (Article 6.7 of the Regulation). They will function as contact points at the national level for the Cybersecurity Competence Community and the ECCC (Article 7.1(a) of the Regulation). They are the interfaces of the cybersecurity community in their country. They will also provide support to carry out actions under this Regulation, and they can pass on financial support to local actors (Article 7.1(f) of the Regulation). Therefore, launching the Network and starting to coordinate its initial activities will be crucial for undertaking the NCCs tasks, thus contributing to the mission of the ECCC and the Network.

With the exception of two MS, all MS have notified to the GB the entities acting as their NCCs. Over the course of 2022, seven dedicated Working Groups of the GB were established with the aim of providing support to the function of the NCCs Network:

- WG1-Community membership and registration.
- WG2-NCCs Reference Manual (working title, pending a final title).
- WG3-NCCs Network functioning.
- WG4-Strategic Agenda.
- WG5-Cyber Skills.
- WG6-Collaboration with Ukraine.
- WG7-Security Operation Centres (SOCs).

During 2023, it is expected that the Network of NCCs will start having regular meetings and interactions, taking over its tasks as set out in the founding Regulation, and functioning as an integrated Network.

Operational support to the mission of the NCCs, and their functioning as a Network, and to the European Cybersecurity Competence Community, will come online in 2023. A dedicated service contract procured through the DEP Call 'Cybersecurity Community Support' (CNECT/2022/OP/0033) will support the activities of the Cybersecurity Competence Community at European level, within the scope and operations of the ECCC and the NCCs Network. The main objectives will be to analyse the Cybersecurity Competence Community, stimulate collaborations, and link the Cybersecurity Competence Community with the ECCC and the NCCs Network.

The cybersecurity community should involve a large, open, and diverse group of actors involved in cybersecurity technology, including in particular research entities, supply/demand-side industries and the public sector. It will provide input to the activities and work plan of the ECCC. And, it will benefit from the community-building activities of the ECCC and the Network.

In the context of the NCCs and the Community, it will be important to increase visibility of EU cybersecurity expertise, products and services. Based on the efforts of the NCCs, the four pilot projects, local/regional efforts in MS, and the "Cyber Atlas" platform, the ECCC will seek to bring together resources and knowledge, on the cybersecurity market and on research in cybersecurity. This will enable the creation of market intelligence and insights, as well as provide an EU-wide overview of the cybersecurity ecosystem. This will be supported also through the Cybersecurity Competence Community service contract described above. This may include the foundations of an "EU cybersecurity market observatory", helping monitor and strengthen EU open strategic autonomy and digital autonomy. This is a challenging aim to be achieved in 2023. Budget-wise, this could be part of the ECCC website infrastructure.

Actions to be undertaken in this activity area during the period which completion is expected over the course of 2023 include the following:

Objective	Expected results
Network of National Coordination Centres	Completion of the setting-up of the Network and smooth functioning as an integrated Network
	Creation of an indicative "service catalogue" for NCCs
	Further definition of modalities of interaction between the ECCC and the Network of NCCs (coordination mechanisms – alignment of activities - Organisation of workshops/recurrent meetings, etc.)
Cybersecurity Competence Community (stakeholders)	Establishment of the Cybersecurity Competence Community
	Establishment of working groups, and support
	Set up an EU "cybersecurity market observatory"

ANNEXES

I. ORGANISATION CHART

Soon after the entering into force of the Regulation, an Interim ED was appointed. The recruitment of the permanent ED was launched and the first staff members were recruited on the basis of the previous Work Programme (SPD 2022-2024). A large number of recruitments, including that of the permanent ED, is expected to be concluded over the course of 2023.

II. RESOURCE ALLOCATION PER ACTIVITY 2023 – 2025

A detailed resource allocation forecast is not available at this stage of establishment and initial operation of the ECCC. The first staff recruitments were launched in 2022 and further staff recruitments will take place over the course of 2023.

III. FINANCIAL RESOURCES 2023 - 2025[34]

Budget Revenue

In accordance with the provisions of the legal framework applicable to the ECCC, for 2023 the only contributor is the EU with the budget planned for Cybersecurity activities in the DEP and covering administrative and operational costs. Contributions from the MS may be taken up with an amendment of the WP and the budget.

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 1: Budget Revenue

REVENUES	Revenues		
	Budget 2023	**Budget Forecast 2024**	**Envisaged 2025**
1 REVENUE FROM FEES AND CHARGES			
2 EU CONTRIBUTION	179 058 443	111 192 243	117 584 478
- Of which Administrative (Title 1 and Title 2)	**2 836 140**	**2 892 863**	**2 950 720**
- Of which Operational (Title 3)	**176 222 303**	**108 299 380**	**114 633 758**
3 THIRD COUNTRIES CONTRIBUTION (incl. EEA/EFTA and candidate countries)	5 246 412	3 257 933	3 445 225

[34] 2023 figures in Tables 2 and 3 are based on the current EU draft budget for 2023.

REVENUES	Revenues		
	Budget 2023	Budget Forecast 2024	Envisaged 2025
- Of which EEA/EFTA (excl. Switzerland)	*5 246 412*	*3 257 933*	*3 445 225*
- Of which candidate countries			
4 OTHER CONTRIBUTIONS			
5 ADMINISTRATIVE OPERATIONS			
6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT			
7 CORRECTION OF BUDGETARY IMBALANCES			
8 INTERESTS GENERATED			
9 UNUSED APPROPRIATIONS FROM PREVIOUS YEARS			
From year N-1			
- Of which Administrative			
- Of which Operational			
From year N-2			
- Of which Administrative			
- Of which Operational			
From year N-3			
- Of which Administrative			
- Of which Operational			
TOTAL	**184 304 855**	**114 450 176**(3)	**121 029 703** (3)

(3) This is based on the 2023 EFTA percentage for DEP: 2,93 %.

Commitment appropriations

Table 2: Commitment appropriations

EXPENDITURE	Commitment appropriations		
	Budget 2023	Budget forecast 2024	Envisaged 2025
TITLE 1 - STAFF EXPENDITURE	**1 778 000**	**1 825 150**	**1 866 176**
Salaries & allowances	1 280 000	1 318 150	1 352 176
- Of which establishment plan posts	*840 000*	*869150*	*894 176*
- Of which external personnel	*440 000*	*449 000*	*458 000*
Expenditure relating to Staff recruitment	62 000	63 000	64 000
Mission expenses	208 000	212 000	216 000
Socio-medical infrastructure	42 000	43 000	43 000
Training	62 000	63 000	64 000
External Services	62 000	63 000	64 000

EXPENDITURE	Commitment appropriations		
	Budget 2023	Budget forecast 2024	Envisaged 2025
Receptions, events and representation	10 000	10 000	10 000
Social welfare	10 000	10 000	10 000
Other Staff related expenditure	42 000	43 000	43 000
TITLE 2 - INFRASTRUCTURE AND OPERATING EXPENDITURE	**1 141 239**	**1 152 474**	**1 171 000**
Rental of buildings and associated costs	156 000	159 000	162 000
Information, communication technology and data processing	62 000	63 000	64 000
Movable property and associated costs	42 000	43 000	43 000
Current administrative expenditure	219 327	224 474	229 000
Postage / Telecommunications	42 000	43 000	43 000
Meeting expenses	42 000	43 000	43 000
Running costs in connection with operational activities	42 000	43 000	43 000
Information and publishing	100 000	102 000	104 000
Studies	124 000	126 000	128 000
Other infrastructure and operating expenditure	311 912	306 000	312 000
TITLE 3 - OPERATIONAL EXPENDITURE	**181 385 616**	**111 472 552**	**117 992 527**
TOTAL	**184 304 855**	**114 450 176**	**121 029 703**

Payment appropriations

Table 3: Payment appropriations

EXPENDITURE	Payment appropriations		
	Budget 2023	Budget forecast 2024	Envisaged 2025
TITLE 1 - STAFF EXPENDITURE	1 778 000	**1 825 150**	**1 866 176**
Salaries & allowances	1 280 000	1 318 150	1 352 176
- Of which establishment plan posts	840 000	*869 150*	*894 176*
- Of which external personnel	440 000	*449 000*	*458 000*
Expenditure relating to Staff recruitment	62 000	63 000	64 000
Mission expenses	208 000	212 000	216 000
Socio-medical infrastructure	42 000	43 000	43 000
Training	62 000	63 000	64 000
External Services	62 000	63 000	64 000
Receptions, events and representation	10 000	10 000	10 000

EXPENDITURE	Payment appropriations		
	Budget 2023	Budget forecast 2024	Envisaged 2025
Social welfare	10 000	10 000	10 000
Other Staff related expenditure	42 000	43 000	43 000
TITLE 2 - INFRASTRUCTURE AND OPERATING EXPENDITURE	**1 141 239**	**1 152 474**	**1 171 000**
Rental of buildings and associated costs	156 000	159 000	162 000
Information, communication technology and data processing	62 000	63 000	64 000
Movable property and associated costs	42 000	43 000	43 000
Current administrative expenditure	219 327	224 474	229 000
Postage / Telecommunications	42 000	43 000	43 000
Meeting expenses	42 000 (1)	43 000	43 000
Running costs in connection with operational activities	42 000	43 000	43 000
Information and publishing	100 000	102 000	104 000
Studies	124 000 (2)	126 000	128 000
Other infrastructure and operating expenditure	311 912	306 000	312 000
TITLE 3 - OPERATIONAL EXPENDITURE	**223 912 363**	**163 638 757**	**140 960 806**
TOTAL	**226 831 602**	**166 616 381**	**143 997 982**

(1) covers innovation
(2) covers audit

Details on the use of financial resources

TITLE 1

Salaries and allowances

This appropriation will cover the cost of remuneration of temporary and contractual staff in accordance with the Staff Regulations. Under this chapter, the costs of the employer's social security contributions in accordance with the applicable Staff Regulations are also covered.

Expenditure relating to staff recruitment

This appropriation is intended to cover the recruitment costs for staff as well as expenditure foreseen in the relevant provisions of the Staff Regulations, e.g. installation allowances for staff changing residence after taking up duties and the daily subsistence allowances due to staff able to prove that they were obliged to change their place of residence after taking up duties. Reimbursement of travel costs and expenses related to the selection process of candidates should be also covered under this item.

Missions' expenses
The missions' appropriation is intended to cover expenditure on transport, the payment of daily mission allowances and the ancillary or exceptional expenses incurred by the staff in the interest of the service in accordance with the Staff Regulations.

Socio-medical infrastructure
This appropriation is intended to cover the costs of the medical check-up of staff and associated analyses required, complementary health insurance and schooling allowances.

TITLE 2
Information communication technology and data processing
This appropriation is intended to cover the installation of the IT infrastructure at the ECCC premises (PCs, networking equipment, software), as well as cybersecurity services, maintenance and IT helpdesk which will be outsourced.

Movable Property
This chapter relates to the initial purchase of furniture and office equipment for the offices of the ECCC.

Current Administrative expenditure
The appropriations are to cover legal costs, costs for Service Level Agreements (SLAs) with other services, insurance and stationery, as well as financial costs (e.g. interest due in case of late payments).

Postage and Telecommunications
These appropriations relate to the costs for internet access as well as other telecom equipment (phones) as needed.

Communication
Activities related to public communication, dissemination and publishing, and in particular:
- Communication products and tools for conferences, info days and workshops
- Website development and consolidation
- General public relations (PR)

Audits
This provision is for external and internal audits needs, legal assistance and other costs.

TITLE 3

In 2023, the EC will launch calls for proposals of the DEP in the area of cybersecurity on behalf of the ECCC.

IV.HUMAN RESOURCES QUANTITATIVE

Table: Statutory staff and SNE

Human Resources	2023	2024	2025
	Authorised Budget	Draft Budget Forecast	Envisaged
Administrators (AD)	10	10	10
Assistants (AST)			
Assistants/Secretaries (AST/SC)			
ESTABLISHMENT PLAN POSTS	**10**	**10**	**10**
Contract Agents (CA)	27	27	27
Seconded National Experts (SNE)	1	1	1
TOTAL STAFF	**38**	**38**	**38**

Staff establishment plan

The table below presents the number of posts in the establishment plans, including the posts assigned to programmes financed outside the EU budget.

Table: Multi-annual staff policy plan 2023, 2024, 2025

Function group and grade	2023		2024		2025	
	Authorised Budget		Draft Budget Forecast		Estimated	
	Permanent posts	Temporary posts	Permanent posts	Temporary posts	Permanent posts	Temporary posts
AD 14		1		1		1
AD 12		2		2		2
AD 11		2		2		2
AD 10						
AD 9						
AD 8		3		3		3
AD 7		2		2		2
AD 6						
AD 5						
AD TOTAL		10		10		10

Function group and grade	2023		2024		2025	
	Authorised Budget		Draft Budget Forecast		Estimated	
	Permanent posts	Temporary posts	Permanent posts	Temporary posts	Permanent posts	Temporary posts
AST/SC TOTAL		0		0		0
TOTAL		10		10		10
GRAND TOTAL	10		10		10	

(1) For the recruitments of AD TA2f, Art 53 CEOS applies. Article 53 CEOS states that the total number of engagements of TA2f at grades AD 9 to AD 12 in an agency cannot exceed 20 % of the total number of engagements of temporary staff to the function group AD, calculated over a five-year rolling period. This limitation does not cover Inter Agency mobility.

External personnel

Contract Agents

Contract agents	2023 estimate	2024estimate	Envisaged 2025
Function Group IV	21	21	21
Function Group III	2	2	2
Function Group II	4	4	4
Function Group I			
TOTAL	27	27	27

Seconded National Experts

Seconded National Experts	2023 estimate	2024 estimate	Envisaged 2025
TOTAL	1	1	1

V.HUMAN RESOURCES QUALITATIVE

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 CAs	Model Decision C(2019)3016	X		
Engagement of TAs	Model Decision C(2015)1509	X		
Middle management staff	Model decision C(2018)2542	X		
Types of post	Model Decision C(2018)8800	X		
Function of Advisor	Model Decision C(2018)2209			

B. Appraisal and reclassification/promotions

		YES	NO	IF NO, WHICH OTHER IMPLEMENTING RULES ARE IN PLACE
Reclassification of TAs	Model Decision C(2015)9560		X	
Reclassification of CAs	Model Decision C(2015)9561		X	
Appraisal of CAs	Model Decision C(2015)1456			
Appraisal of TAs	Model Decision C(2015)1513			

C. Gender representation

While acknowledging the difficulty of reaching gender balance in technical fields such as cybersecurity, the ECCC will take due account in its selection processes of the principle of gender balance in line with the Gender Equality Strategy 2020-2025[35].

[35] 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

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

E. Schooling

Policy to be defined.

VI. ENVIRONMENT MANAGEMENT

Not applicable until hosting building is selected.

VII. BUILDING POLICY

The ECCC headquarters will be located in Bucharest. The initial procedure for the selection of the building which was launched in 2021 was inconclusive. The Romanian Government has offered a new solution for the premises of the ECCC, which are expected to be available to serve the ECCC's needs in 2023. The process will follow the specific provisions regarding building projects as indicated in Article 266 of the Financial Regulation applicable to the general budget of the EU.

VIII. PRIVILEGES AND IMMUNITIES

Not applicable until hosting agreement is adopted.

IX. EVALUATIONS

Not applicable in this Work Programme.

X. STRATEGY FOR THE ORGANISATIONAL MANAGEMENT AND INTERNAL CONTROL SYSTEMS

The GB will in due course adopt the internal control strategy.

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

The ECCC does not receive any form of grant. 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.

Title	Type	Contractor	Status
Service Level Agreement (SLA) and Service Delivery Agreement with DG Budget Implementation and usage of ABAC System	SLA	EUROPEAN COMMISSION / DG BUDG	*Under preparation*
Global SLA with DIGIT	SLA	EUROPEAN COMMISSION / DIGIT	*Signed*
SLA with DG HR	SLA	EUROPEAN COMMISSION / DG HR	*Signed*
SLA with PMO	SLA	EUROPEAN COMMISSION / PMO	*Signed*
SLA with EPSO	SLA	EUROPEAN PERSONNEL SELECTION OFFICE (EPSO)	*Signed*
SLA with EU Agencies Network	SLA	EUROPEAN COMMISSION / SG AGENCES	*Signed*
SLA with ENISA	SLA	ENISA	*Under preparation*
SLA with CERT-EU	SLA	EUROPEAN COMMISSION/ DIGIT	*Under preparation*

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

Not applicable in this Work Programme.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

ANNEX 2

European Cybersecurity Competence Centre Adopted Statement of Estimates 2023 (Budget 2023)

FINANCIAL RESOURCES 2023 - 2025[36]

Budget Revenue

In accordance with the provisions of the legal framework applicable to the ECCC, for 2023 the only contributor is the EU with the budget planned for Cybersecurity activities in the DEP and covering administrative and operational costs. Contributions from the MS may be taken up with an amendment of the WP and the budget.

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 1: Budget Revenue

REVENUES	Revenues		
	Budget 2023	**Budget Forecast 2024**	**Envisaged 2025**
1 REVENUE FROM FEES AND CHARGES			
2 EU CONTRIBUTION	179 058 443	111 192 243	117 584 478
- Of which Administrative (Title 1 and Title 2)	**2 836 140**	**2 892 863**	**2 950 720**
- Of which Operational (Title 3)	**176 222 303**	**108 299 380**	**114 633 758**
3 THIRD COUNTRIES CONTRIBUTION (incl. EEA/EFTA and candidate countries)	5 246 412	3 257 933	3 445 225
- Of which EEA/EFTA (excl. Switzerland)	*5 246 412*	*3 257 933*	*3 445 225*
- Of which candidate countries			
4 OTHER CONTRIBUTIONS			
5 ADMINISTRATIVE OPERATIONS			
6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT			
7 CORRECTION OF BUDGETARY IMBALANCES			
8 INTERESTS GENERATED			

[36] 2023 figures in Tables 2 and 3 are based on the current EU draft budget for 2023.

REVENUES	Revenues		
	Budget 2023	Budget Forecast 2024	Envisaged 2025
9 UNUSED APPROPRIATIONS FROM PREVIOUS YEARS			
From year N-1			
- Of which Administrative			
- Of which Operational			
From year N-2			
- Of which Administrative			
- Of which Operational			
From year N-3			
- Of which Administrative			
- Of which Operational			
TOTAL	**184 304 855**	**114 450 176**(3)	**121 029 703** (3)

(3) This is based on the 2023 EFTA percentage for DEP: 2,93 %.

Commitment appropriations

Table 2: Commitment appropriations

EXPENDITURE	Commitment appropriations		
	Budget 2023	Budget forecast 2024	Envisaged 2025
TITLE 1 - STAFF EXPENDITURE	**1 778 000**	**1 825 150**	**1 866 176**
Salaries & allowances	1 280 000	1 318 150	1 352 176
- Of which establishment plan posts	*840 000*	*869150*	*894 176*
- Of which external personnel	*440 000*	*449 000*	*458 000*
Expenditure relating to Staff recruitment	62 000	63 000	64 000
Mission expenses	208 000	212 000	216 000
Socio-medical infrastructure	42 000	43 000	43 000
Training	62 000	63 000	64 000
External Services	62 000	63 000	64 000
Receptions, events and representation	10 000	10 000	10 000
Social welfare	10 000	10 000	10 000
Other Staff related expenditure	42 000	43 000	43 000
TITLE 2 - INFRASTRUCTURE AND OPERATING EXPENDITURE	**1 141 239**	**1 152 474**	**1 171 000**
Rental of buildings and associated costs	156 000	159 000	162 000
Information, communication technology and data processing	62 000	63 000	64 000
Movable property and associated costs	42 000	43 000	43 000
Current administrative expenditure	219 327	224 474	229 000

EXPENDITURE	Commitment appropriations		
	Budget 2023	Budget forecast 2024	Envisaged 2025
Postage / Telecommunications	42 000	43 000	43 000
Meeting expenses	42 000	43 000	43 000
Running costs in connection with operational activities	42 000	43 000	43 000
Information and publishing	100 000	102 000	104 000
Studies	124 000	126 000	128 000
Other infrastructure and operating expenditure	311 912	306 000	312 000
TITLE 3 - OPERATIONAL EXPENDITURE	**181 385 616**	**111 472 552**	**117 992 527**
TOTAL	**184 304 855**	**114 450 176**	**121 029 703**

Payment appropriations

Table 3: Payment appropriations

EXPENDITURE	Payment appropriations		
	Budget 2023	Budget forecast 2024	Envisaged 2025
TITLE 1 - STAFF EXPENDITURE	1 778 000	**1 825 150**	**1 866 176**
Salaries & allowances	1 280 000	1 318 150	1 352 176
- Of which establishment plan posts	840 000	*869 150*	*894 176*
- Of which external personnel	440 000	*449 000*	*458 000*
Expenditure relating to Staff recruitment	62 000	63 000	64 000
Mission expenses	208 000	212 000	216 000
Socio-medical infrastructure	42 000	43 000	43 000
Training	62 000	63 000	64 000
External Services	62 000	63 000	64 000
Receptions, events and representation	10 000	10 000	10 000
Social welfare	10 000	10 000	10 000
Other Staff related expenditure	42 000	43 000	43 000
TITLE 2 - INFRASTRUCTURE AND OPERATING EXPENDITURE	**1 141 239**	**1 152 474**	**1 171 000**
Rental of buildings and associated costs	156 000	159 000	162 000
Information, communication technology and data processing	62 000	63 000	64 000
Movable property and associated costs	42 000	43 000	43 000
Current administrative expenditure	219 327	224 474	229 000

EXPENDITURE	Payment appropriations		
	Budget 2023	Budget forecast 2024	Envisaged 2025
Postage / Telecommunications	42 000	43 000	43 000
Meeting expenses	42 000 (1)	43 000	43 000
Running costs in connection with operational activities	42 000	43 000	43 000
Information and publishing	100 000	102 000	104 000
Studies	124 000 (2)	126 000	128 000
Other infrastructure and operating expenditure	311 912	306 000	312 000
TITLE 3 - OPERATIONAL EXPENDITURE	**223 912 363**	**163 638 757**	**140 960 806**
TOTAL	**226 831 602**	**166 616 381**	**143 997 982**

(3) covers innovation
(4) covers audit

Details on the use of financial resources

TITLE 1

Salaries and allowances

This appropriation will cover the cost of remuneration of temporary and contractual staff in accordance with the Staff Regulations. Under this chapter, the costs of the employer's social security contributions in accordance with the applicable Staff Regulations are also covered.

Expenditure relating to staff recruitment

This appropriation is intended to cover the recruitment costs for staff as well as expenditure foreseen in the relevant provisions of the Staff Regulations, e.g. installation allowances for staff changing residence after taking up duties and the daily subsistence allowances due to staff able to prove that they were obliged to change their place of residence after taking up duties. Reimbursement of travel costs and expenses related to the selection process of candidates should be also covered under this item.

Missions' expenses

The missions' appropriation is intended to cover expenditure on transport, the payment of daily mission allowances and the ancillary or exceptional expenses incurred by the staff in the interest of the service in accordance with the Staff Regulations.

Socio-medical infrastructure

This appropriation is intended to cover the costs of the medical check-up of staff and associated analyses required, complementary health insurance and schooling allowances.

TITLE 2

Information communication technology and data processing

This appropriation is intended to cover the installation of the IT infrastructure at the ECCC premises (PCs, networking equipment, software), as well as cybersecurity services, maintenance and IT helpdesk which will be outsourced.

Movable Property

This chapter relates to the initial purchase of furniture and office equipment for the offices of the ECCC.

Current Administrative expenditure

The appropriations are to cover legal costs, costs for Service Level Agreements (SLAs) with other services, insurance and stationery, as well as financial costs (e.g. interest due in case of late payments).

Postage and Telecommunications

These appropriations relate to the costs for internet access as well as other telecom equipment (phones) as needed.

Communication

Activities related to public communication, dissemination and publishing, and in particular:

- Communication products and tools for conferences, info days and workshops
- Website development and consolidation
- General public relations (PR)

Audits

This provision is for external and internal audits needs, legal assistance and other costs.

TITLE 3

In 2023, the EC will launch calls for proposals of the DEP in the area of cybersecurity on behalf of the ECCC.