ECCC

EUROPEAN CYBERSECURITY COMPETENCE CENTRE

ECCC 2025 Open Calls - Topics Presentation

DIGITAL-ECCC-2025-DEPLOY-CYBER-08
DIGITAL-ECCC-2025-DEPLOY-CYBER-09
HORIZON-CL3-2025-02-CS-ECCC

Ivan Scannapiecoro
Senior Programme Officer

07/07/2025

#CyberSec_ECCC

Overview

Digital Europe Programme

- Policy Overview
- 2025 Calls – DIGITAL-ECCC-2025-DEPLOY-CYBER-08
  DIGITAL-ECCC-2025-DEPLOY-CYBER-09

Horizon Europe Programme

- Policy overview
- 2025 Call - HORIZON-CL3-2025-02-CS-ECCC

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Overview

Open Calls – focus:

- ✓ *Topics overview*
- ✓ *Timetable and deadlines*
- ✓ *Topics presentation*
- ✓ *Specific topics conditions*
- ✓ *Awards criteria*
- ✓ *Budget categories and cost eligibility*

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Digital Europe Programme

The Digital Europe Programme will reinforce the EU's critical digital capacities by focusing on the key areas of artificial intelligence (AI), cybersecurity, advanced computing, data infrastructure, the deployment of these technologies and their best use for sectors such as energy, climate change and environment, manufacturing, mobility, agriculture and health.

The DEP will strengthen the preparedness and resilience of the key sectors and response actions across the EU to defend against cyber threats.

(Digital Europe Work Programme 2025- 2027)

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

DEP WORK PROGRAMME 2025-2027

Budget Overview

Total: €390 million over 3 years

- €142M: AI & PQC
- €121M: Cyber Solidarity
- €118M: Resilience
- €9M: Support actions

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

DEP WORK PROGRAMME 2025-2027

*Topics and budget are subject to change

	Areas and topics	2025	2026	2027
	New technologies. AI & to post-quantum transition			
2.1	Cybersecure tools, technologies and services relying on AI	X	X	X
2.2	Strengthening cybersecurity capacities of European SMEs with cybersecure AI powered solutions		X	
2.3	Deployment of a European testing infrastructure for the transition to PQC in different usage domains	X		
2.4	Transition to post-quantum Public Key Infrastructures	X		
2.5	Migration of Cyber-Hubs to PQC			X
2.6	Uptake of innovative cybersecurity solutions for SMEs	X		X
	Cyber Solidarity Act Implementation			
2.7	National Cyber Hubs	X	X	
2.8	Cross-Border Cyber Hubs	X		X
2.9	Strengthening the Cyber Hubs ecosystem and enhancing information sharing		X	
2.10	Coordinated preparedness testing and other preparedness actions	X	X	x
2.11	Mutual assistance		X	X
	Additional actions improving EU cyber resilience			
2.12	Enhancing the NCC Network	X	X	x
2.13	Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements		x	X
2.14	Dedicated action to reinforcing hospitals and healthcare providers	X		
2.15	Dual use technologies		x	

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

DIGITAL-ECCC-2025-DEPLOY-CYBER-08

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-PublicPQC

EUR 15 000 000

- **Transition to post-quantum Public Key Infrastructures**

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC

EUR 10 000 000

- **Enhancing the NCC Network**

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CyberHEALTH

EUR 30 000 000

- **Dedicated action to reinforcing hospitals and healthcare providers**

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

DIGITAL-ECCC-2025-DEPLOY-CYBER-08

Timetable and deadlines

Call opening:	**12 June 2025**
Deadline for submission:	**07 October 2025 – 17:00:00 CET (Brussels)**
Evaluation:	**November – December 2025**
Information on evaluation results:	**January – February 2026**
GA signature:	**June – July 2026**

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-PublicPQC

Transition to post-quantum Public Key Infrastructures

Objective

- tackle the challenges of an effective integration of PQC algorithms in Public Key Infrastructures (PKIs), which offers efficient migration strategies and strong business continuity guarantees

Scope

Proposals shall target activities on the following subjects:

- design of digital signature combiners and key encapsulation mechanism combiners.
- the testing of deployment of certificates in protocols that use those certificates.
- the development of novel protocols for Automatic Certificate Management and revocation and of novel protocols for (privacy-friendly) certificate-transparency.
- the development of methods and tools that can be used by experts across various PKI domains, including all aspects of key management of asymmetric systems.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-PublicPQC

- *Indicative duration of the action*: 36 months
- *Type of Action*: Simple Grants - 50% funding rate
- *Grant amount*: EUR 3-4 million
- *Indicative number of projects to be funded*: 3-5
- *Targeted stakeholders*: Stakeholders involved in the Public Key Infrastructures (PKIs) chain, Certificate Authorities (CAs), intermediate CAs and other entities with a focus on cryptography and its standardization activities. The topic targets also other actors in PKI chain and entities that can provide use-case studies and real-world applications for deployment.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC

Enhancing the NCC Network

Based on the financing received in previous years and on the different operational start dates in the Member States, this activity aims to continue providing support for NCCs.

Objectives

- support the operation of the NCCs and enable them to support the cybersecurity community, including SMEs, for the uptake and dissemination of state-of-the-art cybersecurity solutions and strengthen cybersecurity capacities. This could also be achieved by using Financial Support for Third Parties (FSTPs).

- providing support for the uptake of EU cybersecurity technologies and products, commercialisation and scale-up of the European cybersecurity start-up/SME ecosystem, in collaboration and complementarity with the European and ongoing national and regional initiatives, such as accelerator and incubation programmes and technology transfer programmes.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC

Scope

The NCCs should carry out one or more of the following tasks:

- ✓ Act as contact points at the national level for the Cybersecurity Competence Community to support the ECCC in achieving its objectives and missions.
- ✓ Provide expertise and actively contributing to the strategic tasks of the ECCC
- ✓ Promote, encourage and facilitate the participation of civil society and industry in cross-border projects and cybersecurity actions funded through all relevant Union programmes.
- ✓ Provide technical assistance to stakeholders by supporting them in their application phase for projects managed by the ECCC.
- ✓ Seek to establish synergies with relevant activities at national, regional and local levels.
- ✓ Implement specific actions for which grants have been awarded by the ECCC, including through the provision of FSTP; Support the scaling-up of start-ups by finding other funding to implement existing projects.
- ✓ Promote and disseminate the relevant outcomes of the work of the Network and the ECCC
- ✓ Assess requests for becoming part of the Cybersecurity Competence Community by entities established in the same Member State as the NCC.
- ✓ Advocate and promote involvement in the activities arising from the ECCC, the Network of National Coordination Centres, and the Cybersecurity Competence Community.
- ✓ Support the Cybersecurity Competence Community registration (on platforms such as ATLAS) and contribute to the development of suitable community management tools.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC

Scope

In addition, the NCCs could also carry out one or more of the following tasks:

- ✓ Provide support to innovative ideas towards market-readiness.
- ✓ Promote cybersecurity awareness, best practices, and careers in schools, universities, and community events.
- ✓ Strengthen collaboration between institutions for higher education, support activities in primary and secondary levels of education to increase cybersecurity awareness and hygiene.
- ✓ Build stronger partnerships with established SMEs, tech companies, and government agencies to develop and distribute software tools and services that assist in early threat detection, actor identification, and threat evolution monitoring.
- ✓ Organise periodic cybersecurity boot camps, challenges, awareness campaigns and training courses across Europe, specifically for SMEs or students. Organise periodic awareness raising campaigns and cyber exercises to enhance the security and resilience of critical sectors as well as SMEs.
- ✓ Foster a community of cybersecurity professionals who can share their experiences, challenges, and solutions.
- ✓ Support and encourage the uptake of cybersecurity educational policy goals in national (cybersecurity) strategies.
- ✓ Promote safer digital behaviours and more youth considering cybersecurity careers.

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC

- *Indicative duration of the action*: 36 or 48 months
- *Type of Action*: Simple Grants - 50% funding rate
- *Grant amount*: EUR 2-3 million
- *Indicative number of projects to be funded*: 3-5
- *Targeted stakeholders*: National Coordination Centres which have been recognized by the Commission as having the capacity to manage funds to achieve the mission and objectives laid down in the Regulation establishing the ECCC and the Network of National Coordination Centres and other private and other private and public entities in consortium with NCCs, including academia and research entities

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CyberHEALTH

Dedicated action to reinforcing hospitals and healthcare providers

Objective

- strengthen the cybersecurity of hospitals and healthcare providers; ensure that hospitals and healthcare providers can effectively detect, monitor, and respond to cyber threats, particularly ransomware, thereby enhancing the resilience of the European healthcare system.

Scope

The action will support pilot projects bringing together regional and/or national clusters associations of hospitals/healthcare providers and cybersecurity service providers. The pilot projects will:

- *define the state of preparedness* of clusters of hospitals and healthcare providers in the EU, to be able to assess their needs; prepare an *overview of the state-of-the-art cybersecurity solutions and resources* needed for hospitals and healthcare providers to meet the scope of the action.
- *develop technical plans*, tailored to the needs of representative hospitals and healthcare provider
- *conduct a demo implementation* of these technical plans to demonstrate their effectiveness in operations at the stakeholders' sites.
- *serve as demonstration projects* and provide cybersecurity education and training to the staff, enhancing awareness and ensuring best practices in safeguarding sensitive healthcare information.
- undertake *wide dissemination activities of best practices* across the EU

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CyberHEALTH

- *Indicative duration of the action*: 18 or 24 months
- *Type of Action*: Simple Grants - 50% funding rate
- *Grant amount*: EUR 3-5 million
- *Indicative number of projects to be funded*: 6-10
- *Targeted stakeholders*: Regional and/or national clusters associations of hospitals and healthcare providers (such as national healthcare systems, hospitals or associations of hospitals, healthcare providers and/or professional associations of healthcare practitioners), as well as cybersecurity service providers.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

DIGITAL-ECCC-2025-DEPLOY-CYBER-08

Specific topics conditions

- All topics are subject to the provisions of article 12(5) of the Digital Europe Programme Regulation:
  - *participation in any capacity* (as beneficiary, affiliated entity, associated partner, subcontractor or recipient of financial support to third parties) is *limited to entities established in and controlled from* eligible countries
  - *project activities* (included subcontracted work) must take place in eligible countries

- Financial support to third parties is allowed only in topic DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC.

- Consortium composition:
  - For topic DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CYBERHEALTH - *minimum 2 independent applicants* (beneficiaries; not affiliated entities) from at least 2 eligible countries.
  - For topic DIGITAL-ECCC-2025-DEPLOY-CYBER-08-PUBLICPQC, *submissions from consortia*, despite not mandatory, *is strongly advised*.

DIGITAL-ECCC-2025-DEPLOY-CYBER-08

Specific cost eligibility conditions

- Personnel costs:
  - average personnel costs (unit cost according to usual cost accounting practices) : Yes
  - SME owner/natural person unit cost : Yes
- Travel costs:
  - Travel and subsistence unit costs : No (only actual costs)
  - eligible only in EU and EEA countries
- Equipment costs:
  - depreciation (for topic DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC)
  - depreciation + full cost for listed equipment (for topics DIGITAL-ECCC-2025-DEPLOY-CYBER-08-PublicPQC and DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CyberHEALTH)
- Other cost categories: costs for financial support to third parties allowed for grants:
  - for topic DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC: maximum amount per third party EUR 100 000; amounts of more than 60 000 EUR per third party are necessary because the nature of the actions under this call is such that their objectives would otherwise be impossible or overly difficult to achieve;

Type of grant

- Budget-based mixed actual cost grant: actual costs, with unit cost and flat-rate elements
  - ONLY certain types of costs (eligible costs) will be reimbursed
  - costs that were actually incurred for your project (NOT the budgeted costs)
  - For unit costs and flat-rates, the amounts calculated as explained in the Grant Agreement can be charged

DIGITAL-ECCC-2025-DEPLOY-CYBER-08

Awards criteria

Relevance

- Alignment with the objectives and activities
- Contribution to long-term policy and strategic objectives
- Extent to which the project would reinforce and secure the digital technology supply chain in the EU*

Implementation

- Maturity of the proposed action
- Soundness and efficiency of the implementation plan
- Capacity of the applicants or consortium to carry out the proposed work

Impact

- Achievement of the expected outcomes and deliverables, as well as communication and dissemination
- Competitiveness strengthen and contribution to society

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

*Not applicable to topics DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC, DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CyberHEALTH

DIGITAL-ECCC-2025-DEPLOY-CYBER-08

References

- Digital Europe Programme website :
https://digital-strategy.ec.europa.eu/en/activities/digital-programme

- Digital Europe Programme Regulation:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0694&qid=1621344635377

- Funding & tender opportunities portal:
https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/digital

- Call document: Strengthening the Cybersecurity Ecosystem
https://cybersecurity-centre.europa.eu/document/da2e1929-9320-4ae7-97e6-4c3e2ae7de3f_en

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

DIGITAL-ECCC-2025-DEPLOY-CYBER-09

DIGITAL-ECCC-2025-DEPLOY-CYBER-09-CYBERAI — EUR 15 000 000

- Cybersecure tools, technologies and services relying on AI

DIGITAL-ECCC-2025-DEPLOY-CYBER-09-SMEUPTAKE — EUR 15 000 000

- Uptake of innovative cybersecurity solutions for SMEs

DIGITAL-ECCC-2025-DEPLOY-CYBER-09-CYHUBSNAT — EUR 20 000 000

- National Cyber Hubs

DIGITAL-ECCC-2025-DEPLOY-CYBER-09-CYHUBSCRO — EUR 15 000 000

- Cross-Border Cyber Hubs

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-PrepTEST — EUR 10 000 000

- Coordinated preparedness testing and other preparedness actions

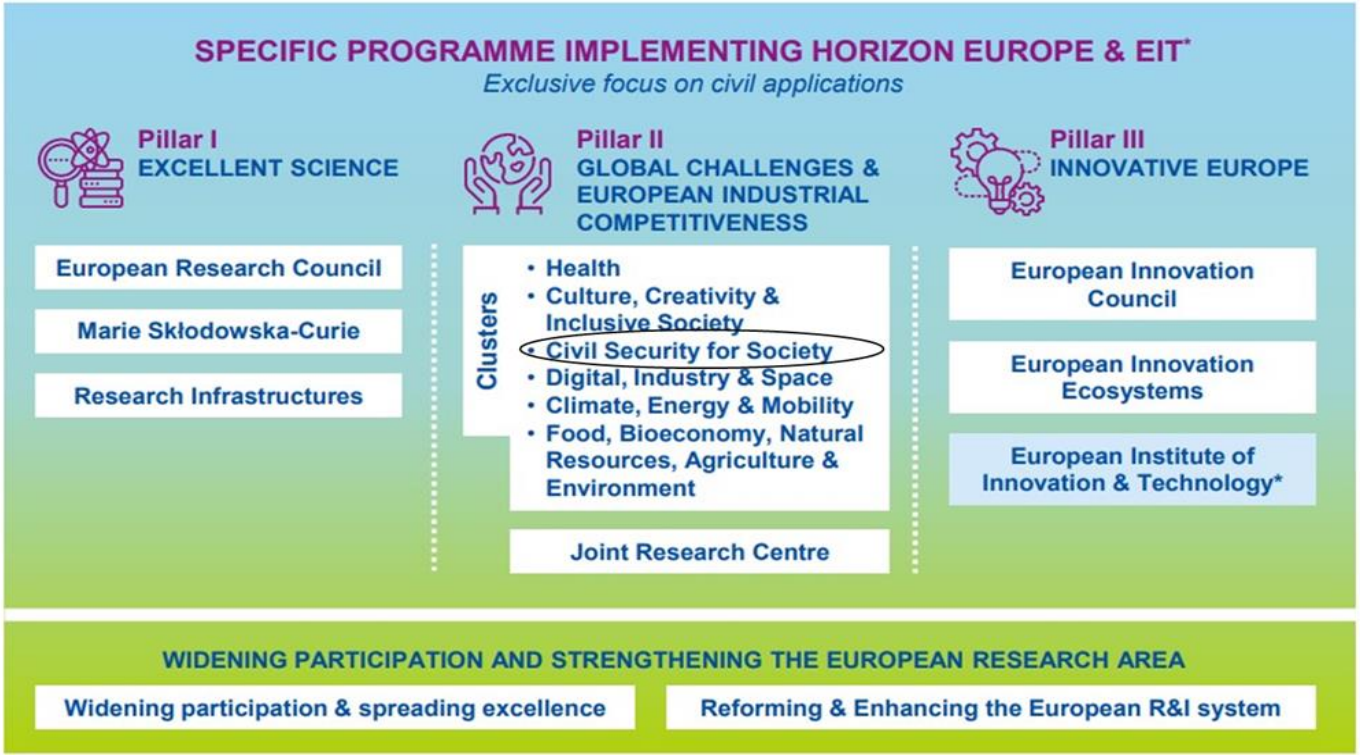
DIGITAL-ECCC-2025-DEPLOY-CYBER-09

Timetable and deadlines

Call opening	**September 2025**
Deadline for submission	**January 2026**
Evaluation	**March - May 2026**
Information on evaluation results	**June 2026**
GA signature (target)	**December 2026**

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Horizon Europe Programme



ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Horizon Europe Programme

Cluster 3 - Civil Security for Society

Cluster 3 provides a research and innovation response to a context of rapidly changing threats and challenges to internal security, the security of citizens, critical infrastructure and the security of society as a whole.

(…) With the aim of creating a secure and trustworthy digital environment, Cluster 3 will invest in cybersecurity R&I to strengthen the EU's resilience, protect its infrastructures, and improve its ability to cope with cyber incidents.

(Horizon Europe Work Programme 2025)

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HE WORK PROGRAMME 2025

Destination - Increased Cybersecurity

Indicative budget: EUR 90.55 million from the 2025 budget

Expected impacts:

· Support the EU's technological capabilities by investing in cybersecurity research and innovation to further strengthen its leadership, strategic autonomy, digital sovereignty and resilience;

· Help protect its infrastructures and improve its ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from cyber and hybrid incidents, especially given the current context of geopolitical change;

· Support European competitiveness in cybersecurity and European strategic autonomy, by protecting EU products and digital supply chains, as well as critical EU services and infrastructures (both physical and digital) (…);

· Encourage the development of the European Cybersecurity Competence Community;

· Particular attention will be given to SMEs (…)by promoting security and privacy 'by design' in existing and emerging technologies.

HORIZON-CL3-2025-02-CS-ECCC

HORIZON-CL3-2025-02-CS-ECCC-01	**EUR 40 000 000**
Generative AI for Cybersecurity applications	
HORIZON-CL3-2025-02-CS-ECCC-02	**EUR 23 550 000**
• New advanced tools and processes for Operational Cybersecurity	
HORIZON-CL3-2025-02-CS-ECCC-03	**EUR 11 000 000**
• Privacy Enhancing Technologies	
HORIZON-CL3-2025-02-CS-ECCC-04	**EUR 4 000 000**
• Security evaluations of Post-Quantum Cryptography (PQC) primitives	
HORIZON-CL3-2025-02-CS-ECCC-05	**EUR 6 000 000**
• Security of implementations of Post-Quantum Cryptography algorithms	
HORIZON-CL3-2025-02-CS-ECCC-06	**EUR 6 000 000**
• Integration of Post-Quantum Cryptography (PQC) algorithms into high-level protocols	

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON-CL3-2025-02-CS-ECCC

Timetable and deadlines

Call opening	**12 June 2025**
Deadline for submission	**12 November 2025** **17:00:00 CET (Brussels)**
Evaluation	**January – February 2026**
Information on evaluation results	**April 2026**
GA signature (target)	**July 2026**

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON-CL3-2025-02-CS-ECCC-01

Generative AI for Cybersecurity applications

Expected outcome

- Projects will develop technologies, tools, processes that reinforce cybersecurity using AI technological components, in particular Generative AI, in line with relevant EU policy, legal and ethical requirements
- Proposals should address at least one of the following expected outcomes:

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

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

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Scope

Proposals addressing expected outcome a)

(a) (i) Advanced threat and anomaly detection and analysis

(a) (ii) Adaptive security measures

(a) (iii) Enhanced authentication and access control.

Proposals addressing expected outcome b)

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

(b) (ii) Adaptation to a dynamic environment.

HORIZON-CL3-2025-02-CS-ECCC-01

- *Type of Action*: Research and Innovation Actions
- *Type of grant*: Budget-based
- *Grant amount*: EUR 12-14 million
- *Indicative number of projects to be funded*: 3
- *Targeted stakeholders*: Participation of SMEs is encouraged

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON-CL3-2025-02-CS-ECCC-02

New advanced tools and processes for Operational Cybersecurity

Scope

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

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

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON-CL3-2025-02-CS-ECCC-02

Expected outcome

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

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

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON-CL3-2025-02-CS-ECCC-02

- *Type of Action*: Innovation Actions
- *Grant amount*: EUR 4,5-6 million
- *Type of grant*: Lump Sum
- *Indicative number of projects to be funded*: 4
- *Targeted stakeholders*: the participation of the following types of entities is highly encouraged and would be considered an asset:
    - innovative European cybersecurity start-ups and SMEs with a proven track-record in cybersecurity innovation at EU level,
    - European start-ups and SMEs that can demonstrate established operational cooperation with relevant National Cybersecurity Authorities,
    - European start-ups and SMEs that have received equity investments by national,
    - European or private Venture Capital funds for cybersecurity activities

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON-CL3-2025-02-CS-ECCC-03

Privacy Enhancing Technologies

Scope

Consortia are encouraged to propose solutions that can improve the usability and effectiveness of different Privacy-enhancing technologies (PETs) in realistic environment and to investigate their integration within common European data spaces. The inclusion of agile schemes designed in a modular way to support the transition to post-quantum PETs and the design, improvement and security analysis of quantum-resistant PETs is welcome, in light of the advances of quantum technologies.

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

HORIZON-CL3-2025-02-CS-ECCC-03

Expected outcome

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

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

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON-CL3-2025-02-CS-ECCC-03

- *Type of Action*: Research and Innovation Actions
- Type of grant: Lump Sum
- *Grant amount*: EUR 3-4 million
- *Indicative number of projects to be funded*: 3
- *Targeted stakeholders*: consortia should seek to intertwine interdisciplinary expertise and resources from industry stakeholders, service providers, and end-users. The engagement of SMEs is encouraged, alongside the inclusion of legal proficiency to ensure regulatory compliance, including GDPR adherence

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON-CL3-2025-02-CS-ECCC-04

Security evaluations of Post-Quantum Cryptography (PQC) primitives

Scope

Proposals on the assessment of the security of post-quantum primitives, via studies focused on eventual quantum algorithms with demonstrable speed-up, eventually also in combination with AI, or on solely AI-based approaches, are welcome. The security of lattice and code-based PQC algorithms may be prioritized, but tackling other mathematical problem classes is not excluded. As the unprecedented computational power of quantum computing can greatly enhance AI capabilities, combination of different approaches may also be considered.

Projects should lead to identification of vulnerabilities of current post-quantum cryptographic building blocks and to practical recommendations for parameters for the design of post-quantum cryptosystems with improved security against quantum attacks and future advances in code-breaking and AI.

HORIZON-CL3-2025-02-CS-ECCC-04

Expected outcome

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

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

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON-CL3-2025-02-CS-ECCC-04

- *Type of Action*: Research and Innovation Actions
- *Grant amount*: EUR 2-3 million
- *Type of grant*: Lump Sum
- *Indicative number of projects to be funded*: 2
- *Targeted stakeholders*: consortia with team of applicants with background in post-quantum cryptography and in quantum computing are particularly encouraged.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON-CL3-2025-02-CS-ECCC-05

Security of implementations of Post-Quantum Cryptography algorithms

Scope

Proposals are welcome on developing solutions that protect against implementation attacks, at reasonable costs and minimizing the loss of performance while maintaining the required security, as well as on the analysis of new attacks or combinations of attacks, also powered by the use of AI, for security-by-design approaches when designing Post Quantum Cryptographic systems.

Activities can also lead to the development of testing methodologies and frameworks for automated security evaluations for correctness and resistance to remote side-channel attacks for regular software and for correctness and resistance to a broad range of implementation attacks for embedded software and hardware.

HORIZON-CL3-2025-02-CS-ECCC-05

Expected outcome

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

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

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON-CL3-2025-02-CS-ECCC-05

- *Type of Action*: Research and Innovation Actions
- *Type of grant*: Lump Sum
- *Grant amount*: EUR 2-3 million
- *Indicative number of projects to be funded*: 2
- *Targeted stakeholders*: general conditions apply

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON-CL3-2025-02-CS-ECCC-06

Integration of Post-Quantum Cryptography (PQC) algorithms into high-level protocols

Scope

Activities should target one or multiple relevant high-level protocols and produce their post-quantum versions.

Typically, this can be achieved through combining current and post-quantum solutions for backward compatibility. Atypical solutions with equivalent security are also welcome.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON-CL3-2025-02-CS-ECCC-06

Expected outcome

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

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

HORIZON-CL3-2025-02-CS-ECCC-06

- *Type of Action*: Research and Innovation Actions
- *Grant amount*: EUR 2-3 million
- *Type of grant*: Lump Sum
- *Indicative number of projects to be funded*: 2
- *Targeted stakeholders*: consortia composed by actors of different nature, such as, for example, research institutions, relevant public entities, and industry to ensure that PQC solutions meet real-world security demands and are robustly tested across various applications are welcome.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON-CL3-2025-02-CS-ECCC

Specific topics conditions

- For topics HORIZON-CL3-2025-02-CS-ECCC-01 and HORIZON-CL3-2025-02-CS-ECCC-02, participation is limited to legal entities established in Member States and Associated Countries. In terms of control conditions, entities established in an eligible country listed above, but which are directly or indirectly controlled by a non-eligible country or by a non-eligible country entity, shall not participate in the action.

- For topics HORIZON-CL3-2025-02-CS-ECCC-04, HORIZON-CL3-2025-02-CS-ECCC-05 and HORIZON-CL3-2025-02-CS-ECCC-06, participation is limited to legal entities established in Member States and Associated Countries and OECD countries. In terms of control conditions, entities established in an eligible country listed above, but which are directly or indirectly controlled by a non-eligible country or by a non-eligible country entity, shall not participate in the action.

- For topic HORIZON-CL3-2025-02-CS-ECCC-03, the following Eligibility exceptions apply: *subject to restrictions for the protection of European communication networks*

Awards criteria

Excellence

- Clarity and pertinence of the project's objectives, and the extent to which the proposed work is ambitious, and goes beyond the state-of-the-art.
- Soundness of the proposed methodology, including the underlying concepts, models, assumptions, inter-disciplinary approaches, appropriate consideration of the gender dimension in research and innovation content, and the quality of open science practices including sharing and management of research outputs and engagement of citizens, civil society and end users where appropriate.

Impact

- Credibility of the pathways to achieve the expected outcomes and impacts specified in the work programme, and the likely scale and significance of the contributions due to the project.
- Suitability and quality of the measures to maximize expected outcomes and impacts, as set out in the dissemination and exploitation plan, including communication activities.

Quality and efficiency of the implementation

- Quality and effectiveness of the work plan, assessment of risks, and appropriateness of the effort assigned to work packages, and the resources overall.
- Capacity and role of each participant, and extent to which the consortium as a whole brings together the necessary expertise.

HORIZON-CL3-2025-02-CS-ECCC

References

- Horizon Europe Programme website : https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en

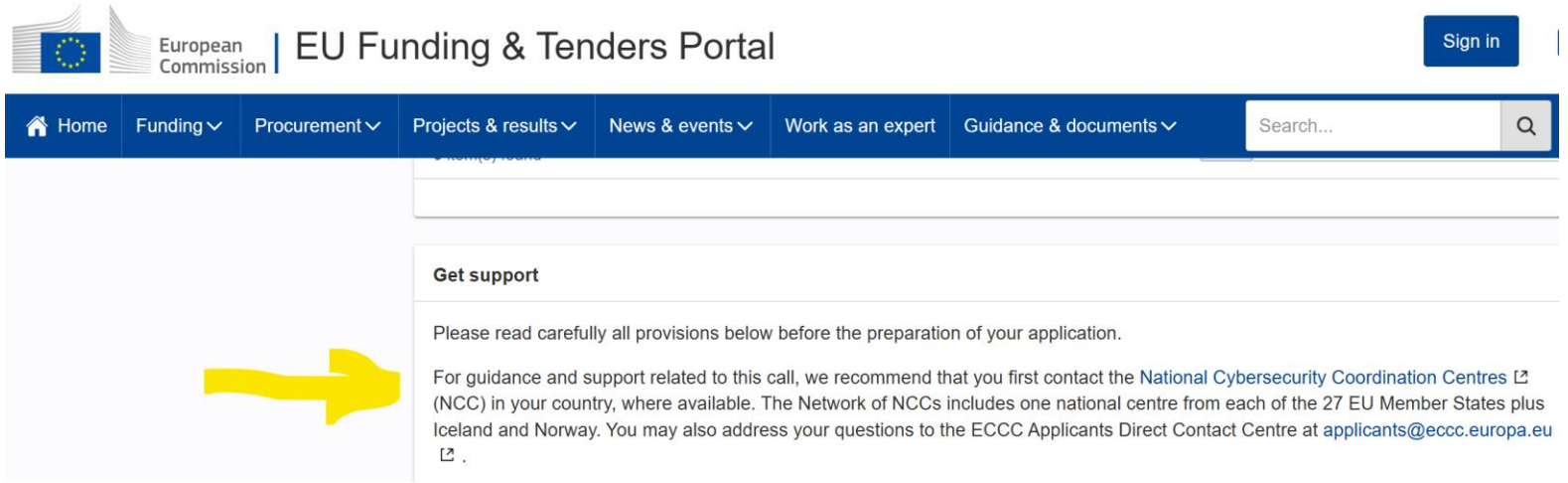
- Horizon Europe Work Programmes: https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/horizon-europe-work-programmes_en

- Funding & tender opportunities portal: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/horizon

- HORIZON-CL3-2025-02-CS-ECCC Call: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/calls-for-proposals

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Help!



ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Q & A

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

Follow us

cybersec_eccc

cybersec_eccc

cybersec_eccc

CyberECCC

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Europe digitally secured