ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

ECCC - Horizon Europe programme and funding opportunities for projects in the field of cybersecurity

Polyvios Hadjiyiangou, Head of Operations

Second national
NCC-HR conference

Overview

Horizon Europe Programme - HORIZON-CL3-2025-02-CS-ECCC

- *Topics overview*
- *Awards criteria*
- *Timetable and deadlines*

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HE and DEP: strengthen Europe's cyber-resilience and strategic autonomy

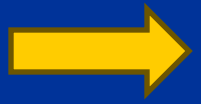
HE provides the *"what's next"*: new knowledge, concepts & prototypes

DEP delivers the *"what's now"*: operational rollout & impact at scale

Horizon Europe (HE)

Focus: Research & Innovation

- Supports cutting-edge cybersecurity research
- Develops next-gen tools, technologies, and methodologies
- Funds long-term innovation projects



Digital Europe Programme (DEP)

Focus: Deployment & Capacity Building

- Scales up tested solutions from HE into real-world use
- Funds cybersecurity infrastructure and training
- Supports digital skills development and cybersecurity operations
- Builds EU-wide cybersecurity capabilities (e.g., SOCs, cyber-hubs)

ECCC facilitates the use of results from research and innovation projects in actions related to the deployment of cybersecurity products, services and processes,

Call - Increased Cybersecurity
HORIZON-CL3-2025-02-CS-ECCC

HORIZON-CL3-2025-02-CS-ECCC-01 • Generative AI for Cybersecurity applications	EUR 40.000.000
HORIZON-CL3-2025-02-CS-ECCC-02 • New advanced tools and processes for Operational Cybersecurity	EUR 23.550.000
HORIZON-CL3-2025-02-CS-ECCC-03 • Privacy Enhancing Technologies	EUR 11.000.000
HORIZON-CL3-2025-02-CS-ECCC-04 • Security evaluations of Post-Quantum Cryptography (PQC) primitives	EUR 4.000.000
HORIZON-CL3-2025-02-CS-ECCC-05 • Security of implementations of Post-Quantum Cryptography algorithms	EUR 6.000.000
HORIZON-CL3-2025-02-CS-ECCC-06 • Integration of Post-Quantum Cryptography (PQC) algorithms into high-level protocols	EUR 6.000.000

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Horizon Europe: Expected outcome and Scope

Expected outcome: What difference will your project make if it's successful?

Think of the scope as the 'space to innovate within' — it's broad enough to allow creativity, but specific enough to guide applicants in the right direction.

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

Expected Outcome

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.

Indicative number of projects to be funded: 3

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

Scope (expected outcome a)

- Generative AI models to identify anomalies and deviations from normal behaviour.
- Support professionals in detecting and responding to generative AI threats.
- Enable real-time adaptation to emerging threats.
- Overcome limits of static rules and manual intervention.
- Improve resilience of authentication and access control systems.

Indicative number of projects to be funded: 3

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

Scope (expected outcome b)

- Tools powered by Generative AI to analyse and facilitate the application of national and EU regulation.
- Focus on the Artificial Intelligence Act, NIS2 Directive, and Cyber Resilience Act.
- Adaptation to a dynamic environment faced by companies, public sector and organisations.
- Variety of rules at sectorial, national or European level to be considered.
- Frequent change management and updates in ICT systems in organisations.
- Compliance continuum within organisations otherwise limited in time when driven by human intervention only.

Indicative number of projects to be funded: 3

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

- Respect Trustworthy and Responsible AI principles and data privacy.
- Demonstrate EU added value by fostering EU technology and use of open-source technologies when feasible.
- Exploit available EU data (Data Spaces, federated data etc).
- Define KPIs with baseline targets to measure progress and advancement to the state-of-the-art.
- Appropriately document technologies and tools to support take-up and replicability.
- Pay special attention to the Intellectual Property dimension and the usability of outcomes after project completion.

Indicative number of projects to be funded: 3

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

Expected Outcome

- Enhanced Situational Awareness via Cyber Threat Intelligence and supply chain risk assessments
- Tools for preparedness against Cyber and Hybrid Threats in ICT and OT, incl. exercises
- Expanded SOC/CSIRT functionality for detection, response, and remediation
- Testing facilities for cybersecurity tools, incl. digital twins for NIS2 entities
- Cross-sector/cross-border cyber crisis management frameworks and tools
- Tools for operational cooperation (CSIRT, EU-CyCLONe); extendable to NIS2 entities

projects to be funded:4

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

Scope

- Demonstration of developed frameworks, tools, services, and processes through pilot implementations.
- 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.
- Participation of innovative European cybersecurity start-ups and SMEs with a proven track-record in cybersecurity innovation at EU level is highly encouraged.

projects to be funded:4

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

Expected outcome

- Development of robust, scalable, and reliable technologies to uphold privacy within federated and secure data sharing frameworks.
- Integration of privacy-by-design at the core of software and protocol development processes.
- Development of privacy preserving approaches for data sharing solutions, including privacy-preserving cyber threat information sharing.
- Contribution towards the advancement of GDPR-compliant European data spaces for digital services and research.
- Development of blockchain-based and decentralised privacy-enhancing technologies to preserve data confidentiality, integrity, and authenticity.
- Investigating the usability and user experience of privacy-enhancing technologies.

projects to be funded:4

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

Scope

- Protecting personal data and ensuring privacy is fundamental for our society.
- Privacy-preserving techniques minimise data collection and use advanced cryptographic methods.
- Personal data raises concerns over breaches, jeopardising privacy, societal well-being, and economic stability.
- PETs hold promise but require further refinement and rigorous testing.
- Consortia should improve PETs' usability in realistic environments and integrate them into European data spaces.
- Proposals must ensure GDPR adherence and address regulatory hurdles.

Indicative number of projects to be funded: 3

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

Expected Outcome

- Quantum hardness of mathematical problem classes.
- Quantum speed-up for lattice-based, code-based, and other problem-classes.
- High-level quantum programming for solving cryptographic problems.
- Testing robustness of cryptosystems against quantum attackers.
- AI-based approaches to discover vulnerabilities.
- Parameter suggestions for post-quantum cryptographic building blocks.

Indicative number of projects to be funded: 2

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

Scope

- PQC security is based on problems believed to be intractable for classical and quantum computers.
- Assessing the quantum security of post-quantum primitives is fundamental.
- A quantum speed-up would require reassessment of cryptosystem security.
- Quantum attackers fail due to lack of efficient implementations and hardware.
- AI-based approaches may help discover vulnerabilities in some schemes.
- Projects should give practical recommendations to improve post-quantum security.

projects to be funded:2

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

Expected Outcome

- Design and implementations of Post-Quantum Cryptography (PQC) algorithms resistant to side-channel and fault attacks
- Optimised countermeasures with a balanced trade-off between security, performance, and costs
- Recommendations on implementing countermeasures for a broad range of attacks
- Identification of available and necessary hardware
- Analysis of new attacks or combinations of attacks, also eventually enhanced by AI
- Design of automated security evaluations for PQC implementations

Indicative number of projects to be funded: 2

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

Scope

- Security of PQC implementations is vital for confidentiality, integrity, authenticity and availability.
- Implementation attacks (e.g. side-channel, fault attacks) pose significant threats to software and hardware.
- Countermeasures may cause substantial resource overhead and impact run-time and memory consumption.
- Resistance to implementation attacks is an increasingly common concern among customers.
- Evaluating security against side-channel and fault attacks is crucial, given the proven vulnerabilities.
- Proposals welcome for solutions protecting against implementation attacks, minimising loss of performance.

Indicative number of projects to be funded: 2

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

Expected Outcome

- 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;
- 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.

Indicative number of projects to be funded: 2

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

Scope

- Transition requires changing RSA (Rivest–Shamir–Adleman) and ECC (Elliptic Curve Cryptography).
- Post-quantum cryptography being added to TLS (Transport Layer Security).
- More protocols must become quantum-ready.
- IoT, cloud, automotive face bandwidth/time limits.
- Embedded hardware apps (e.g. secure elements, Two-Factor Authentication, MFA – Multi-Factor Authentication) need early migration.
- Target high-level protocols for post-quantum versions.

Indicative number of projects to be funded: 2

Award criteria

Criterion	Sub-criteria
Excellence	• Clarity and pertinence of the objectives- • Soundness of the proposed methodology • Ambition and innovation potential (beyond the state of the art)
Impact	• Credibility of the pathways to achieve the expected outcomes and impacts • Suitability of the proposed measures to maximise impact (including dissemination, exploitation, communication)
Quality and Efficiency of Implementation	• Quality of the work plan, including tasks, resources and timing • Quality of the consortium and suitability of participants- • Appropriateness of the management structures and procedures, risk management

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Specific eligibility restrictions

In terms of General Eligibility conditions to which your question is related, they are described in General Annex B [link].

Most of the topics part of the call in subject impose specific eligibility **restrictions** in terms of

- **Security** - In order to achieve the expected outcomes, and safeguard the Union's strategic assets, interests, autonomy, and security - by listing the **eligible countries where the participants have to be established**
- **Control** - In order to guarantee the protection of the strategic interests of the Union and its Member States - by conditioning the **countries where the entities controlling the partners are established**.

These restrictions slightly vary between the topics.

Read the Work Programme carefully

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Call indicative timelines 2025-2026

Call process	Horizon Europe
Call opening	June 2025
Deadline for submission	November 2025
Evaluation	January 2026 – February 2026
Information on evaluation results	April 2026
GA signature (target)	July 2026

Keep in touch

 ECCC Newsletter

 ECCC LinkedIn

 ECCC Twitter/X

 ECCC Instagram

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Thank you!

Europe digitally secured