ECCC

EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Information on current Nordic and Baltic participation in EU funded cybersecurity projects and EU calls for application

Ivan SCANNAPIECORO
Head of Sector - Community and Competence
23/04/2026

#CyberSec_ECCC

Nordic-Baltic region

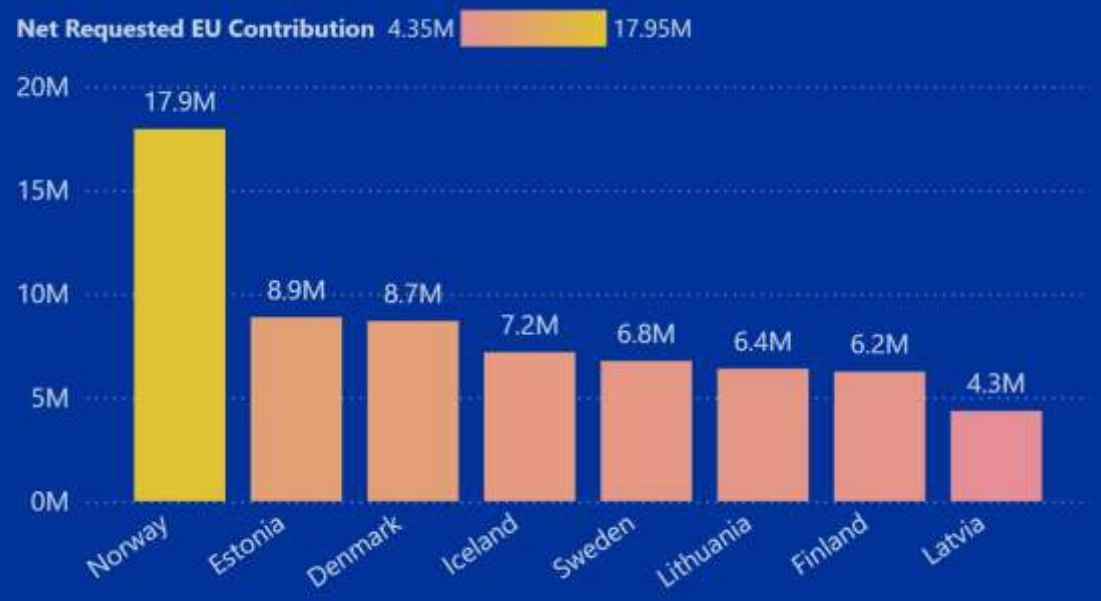
It is meant:

- Norway
- Sweden
- Denmark
- Finland
- Iceland
- Estonia
- Latvia
- Lithuania

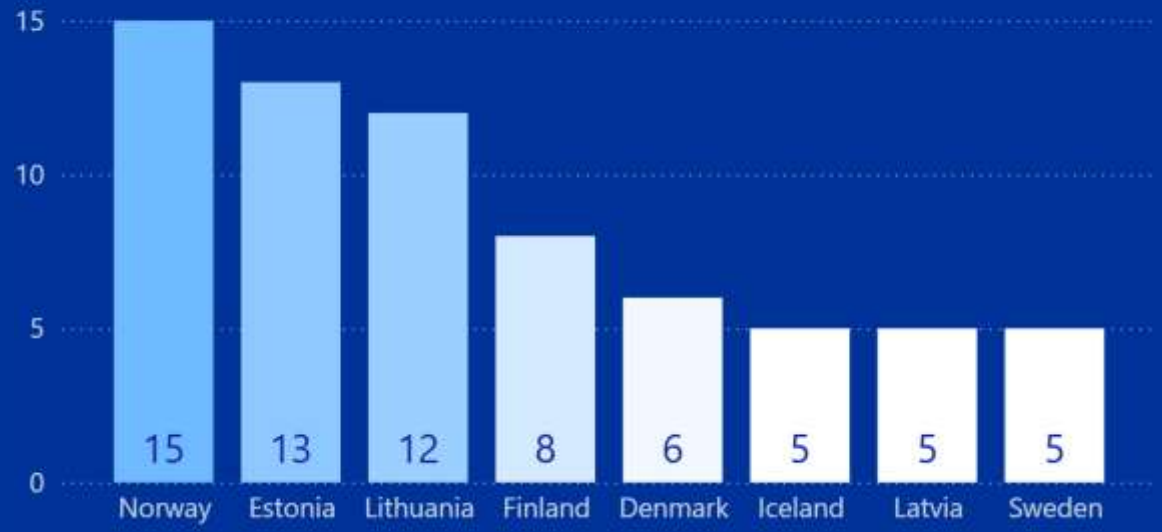
ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Cybersecurity - DEP + HE

EU Contribution per Country



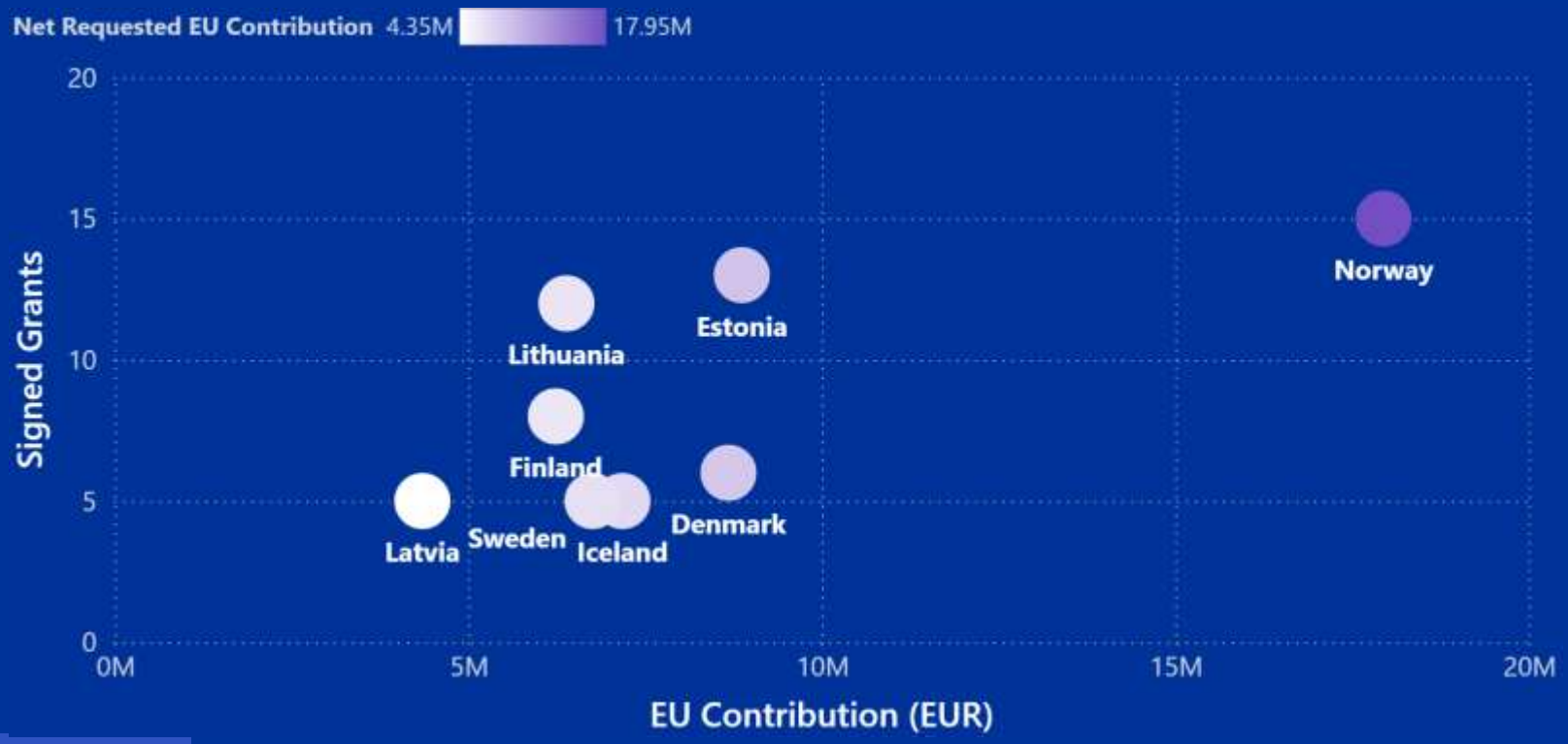
Number of Signed Grants per Country



ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Cybersecurity - DEP + HE

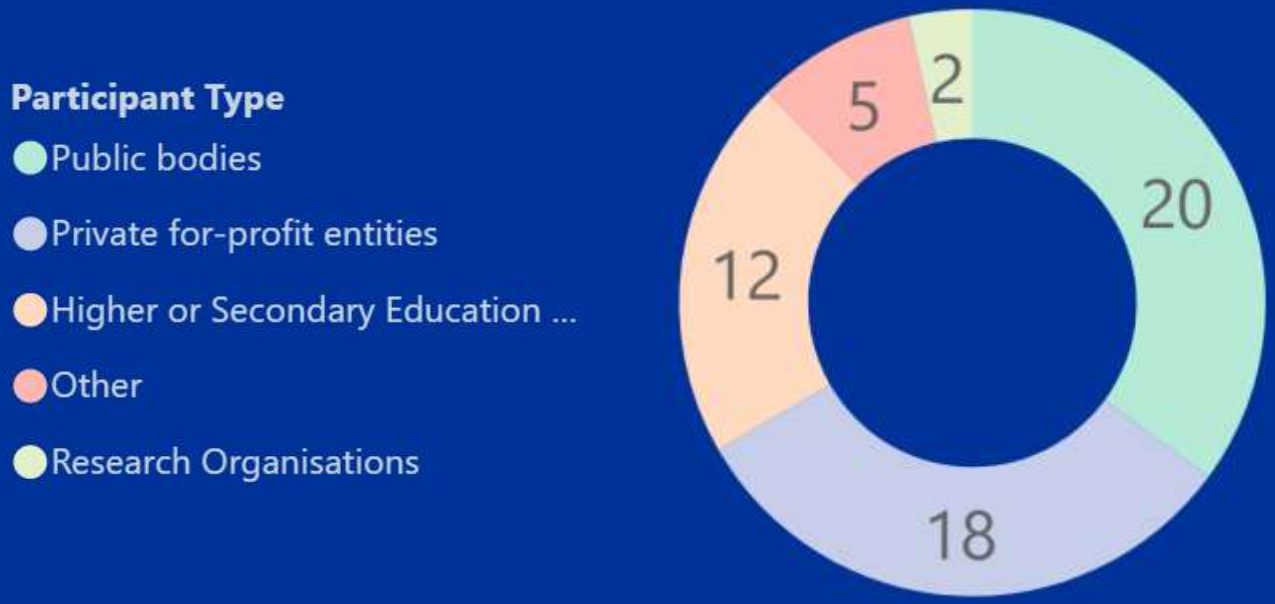
EU Contribution/Signed Grants per country



ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Cybersecurity - DEP

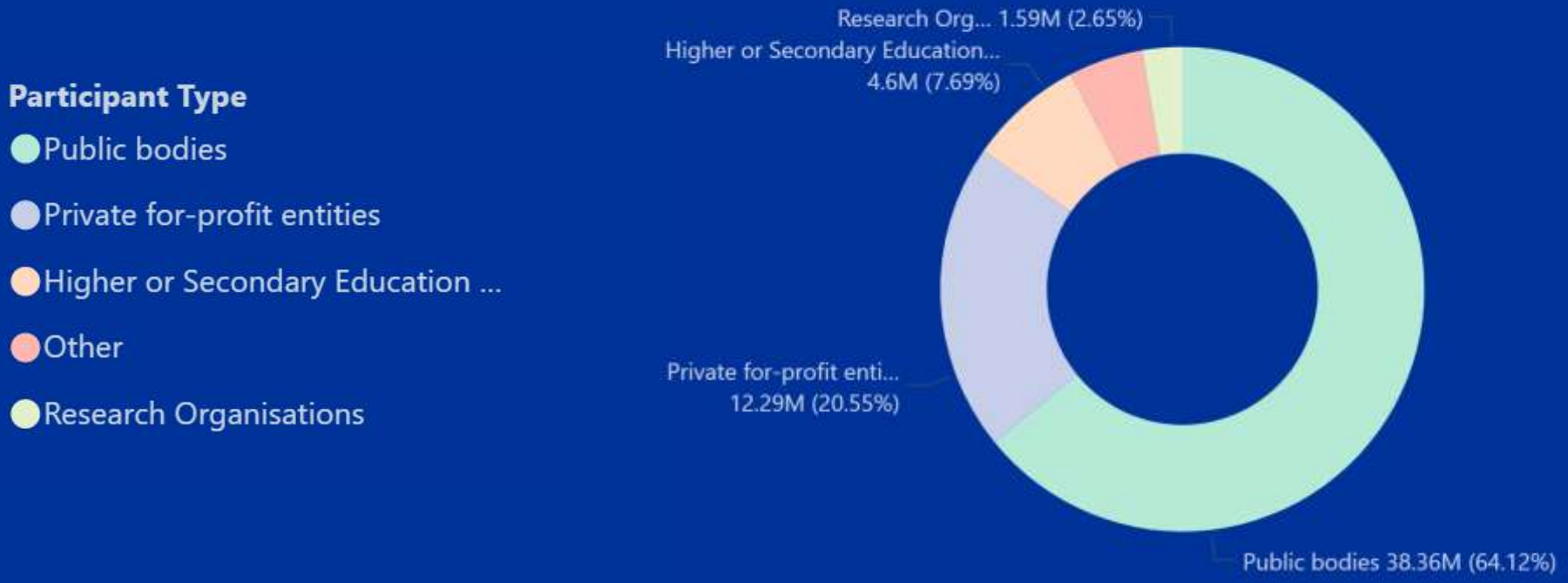
Unique participants type



ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Cybersecurity - DEP

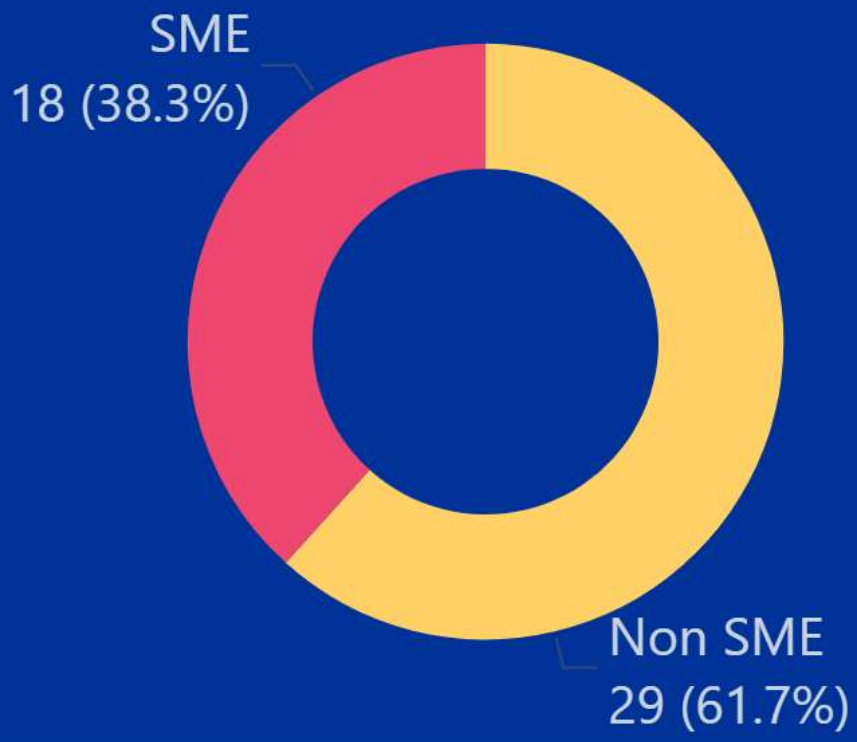
Participant type by EU Contribution



ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Cybersecurity - DEP

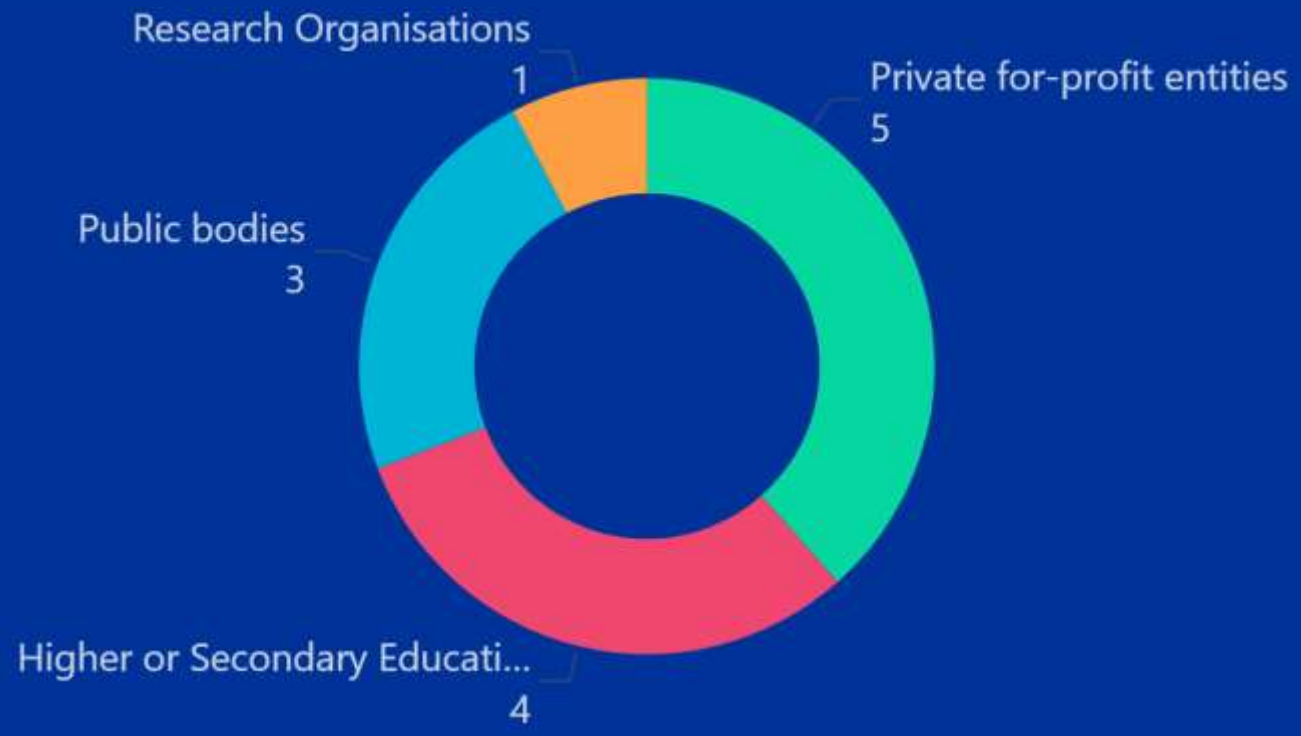
Unique Participants by SME/non SME



ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Cybersecurity – Horizon Cluster 3

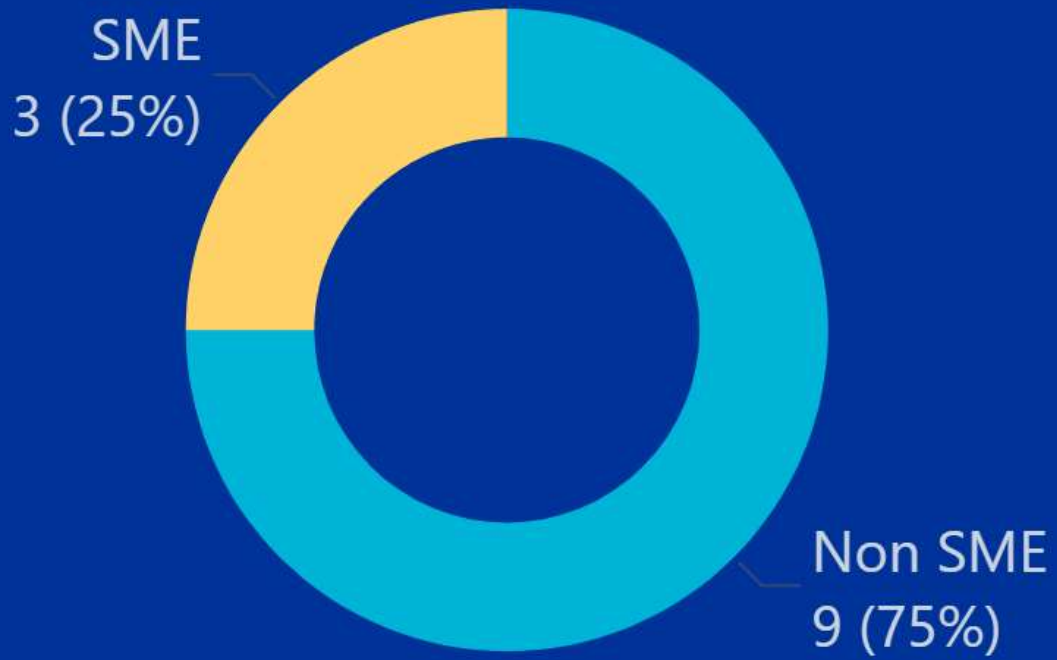
Unique Participants by type



ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Cybersecurity – Horizon Cluster 3

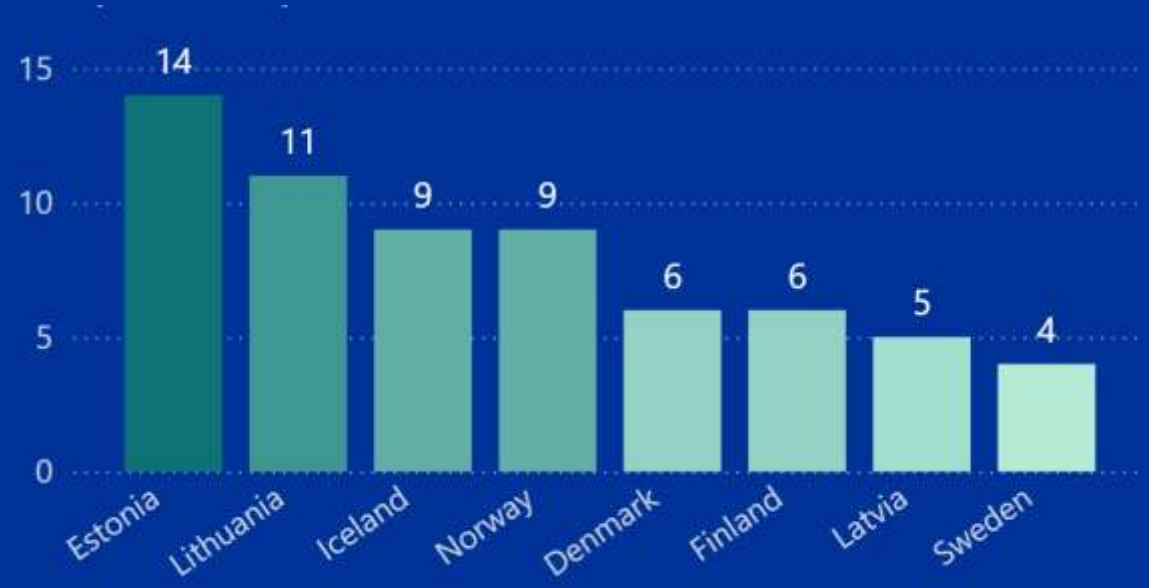
Unique Participants by SME/non SME



ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Cybersecurity DEP + HE - Participation per country

Unique participants per country



Total number of participation per country

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Proposals/Applicants statistics

293

Proposals Eligible

41,86% of All

Proposals meeting the requirements to become eligible for a grant.

43

Proposals Retained

14,68% Success Rate Proposals

600

Applications Eligible

8,43% of All

Number of organizations being part of eligible proposals. A single organization involved in N proposals is counted N times

91

Applications Retained

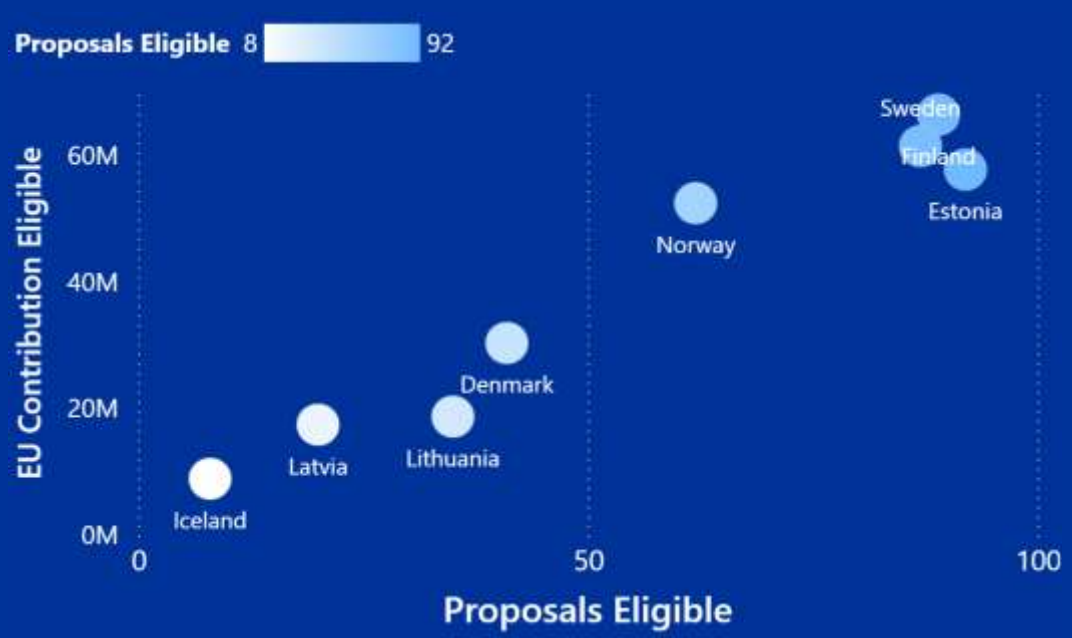
15,17% Success Rate

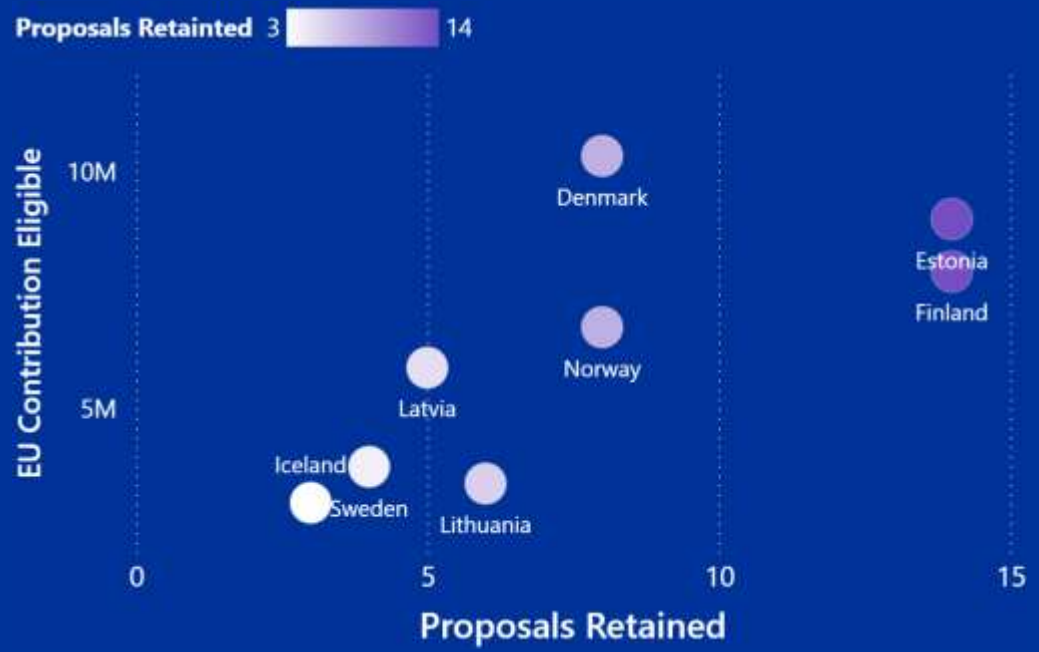
Number of organizations being part of retained proposals. A single organization involved in N proposals is counted N times

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Data scope: limited to the following calls: DIGITAL-ECCC-2024-DEPLOY-CYBER-06, DIGITAL-ECCC-2024-DEPLOY-CYBER-07, DIGITAL-ECCC-2024-DEPLOY-NCC-06, DIGITAL-ECCC-2025-DEPLOY-CYBER-08, HORIZON-CL3-2024-CS-01, and HORIZON-CL3-2025-02-CS-ECCC.

EU Contribution/Proposals Eligible,Retained

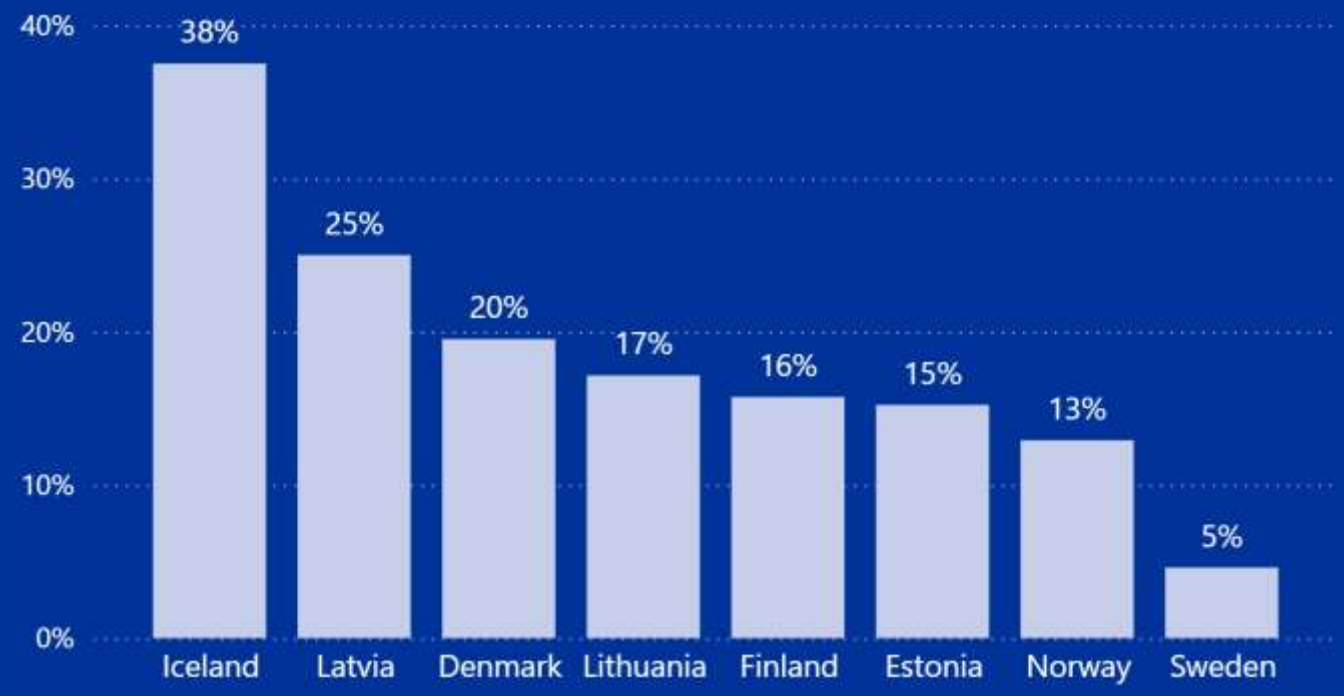




ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Charts based exclusively on data from the following calls: DIGITAL-ECCC-2024-DEPLOY-CYBER-06, DIGITAL-ECCC-2024-DEPLOY-CYBER-07, DIGITAL-ECCC-2024-DEPLOY-NCC-06, DIGITAL-ECCC-2025-DEPLOY-CYBER-08, HORIZON-CL3-2024-CS-01, and HORIZON-CL3-2025-02-CS-ECCC.

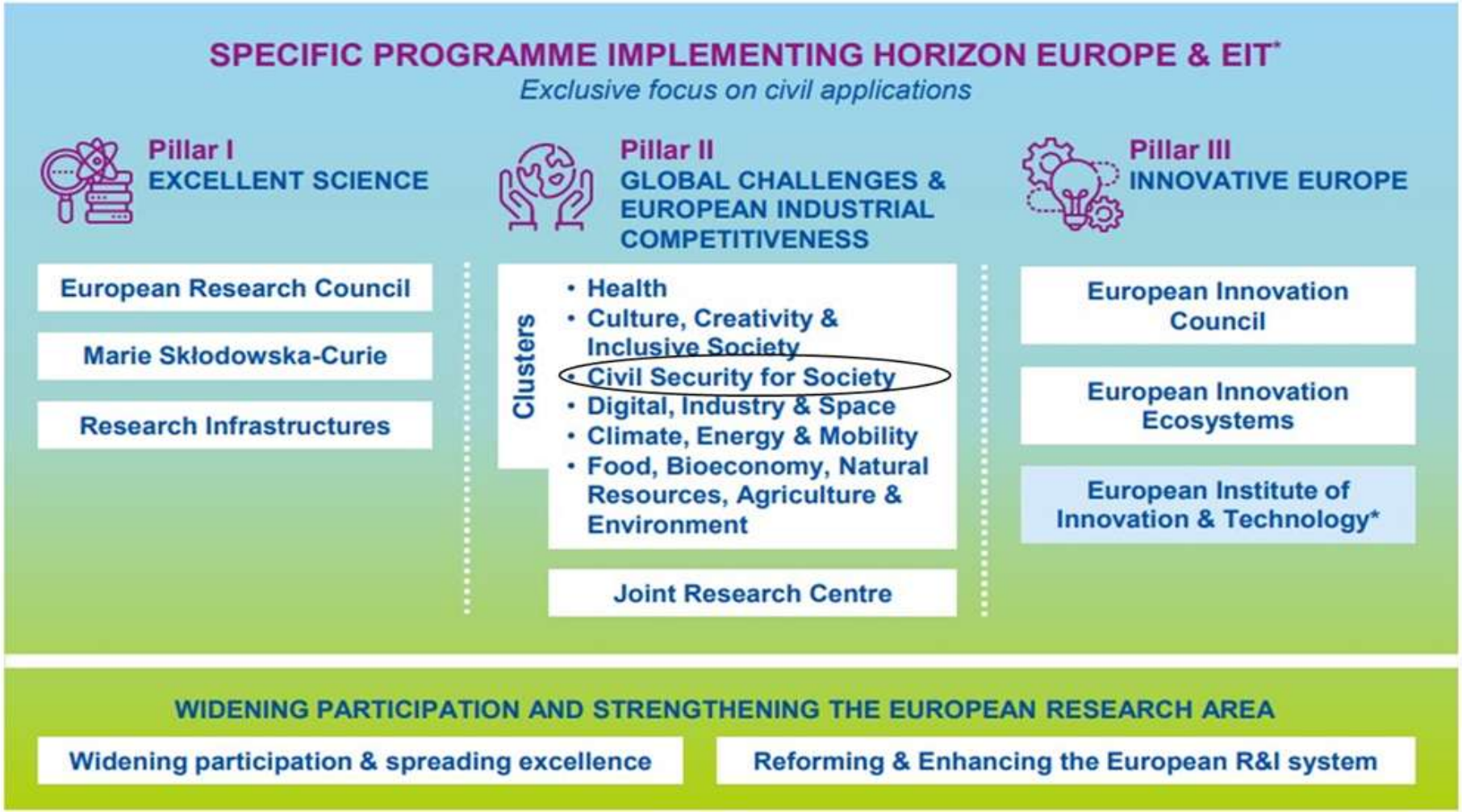
Success Rate for Proposals (by country)



ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Charts based exclusively on data from the following calls: DIGITAL-ECCC-2024-DEPLOY-CYBER-06, DIGITAL-ECCC-2024-DEPLOY-CYBER-07, DIGITAL-ECCC-2024-DEPLOY-NCC-06, DIGITAL-ECCC-2025-DEPLOY-CYBER-08, HORIZON-CL3-2024-CS-01, and HORIZON-CL3-2025-02-CS-ECCC.

HORIZON EUROPE PROGRAMME



ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON EUROPE WORK PROGRAMME 2026-2027

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.

(Horizon Europe Work Programme 2026-2027)

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON EUROPE WORK PROGRAMME 2026-2027

Destination - Cybersecurity

Actions proposed:

- *Are designed to reinforce the EU's ability to detect, prevent, and respond to cyber threats, including those targeting critical infrastructure.*
- *Contribute to Europe's open strategic autonomy by supporting the development of trustworthy digital infrastructures, emerging technologies, cybersecurity capabilities, and secure supply chains.*

Expected impacts:

Increased cybersecurity and a more secure online environment by developing and using effectively EU and Member States' capabilities in digital technologies supporting protection of data and networks aspiring to technological sovereignty in this field, while respecting privacy and other fundamental rights; this should contribute to secure services, processes and products, as well as to robust digital infrastructures capable to resist and counter cyber-attacks and hybrid threats.

(Horizon Europe Work Programme 2026-2027)

HORIZON-CL3-2026-02-CS-ECCC

Timetable and deadlines

Call opening	**09 March 2026**
Deadline for submission	**15 September 2026** **17:00:00 CET (Brussels)**
Evaluation	**November 2026**
Information on evaluation results	**January 2027**
GA signature (target)	**May 2027**

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON-CL3-2026-02-CS-ECCC

HORIZON-CL3-2026-02-CS-ECCC-01 (RIA)

EUR 20 000 000

Approaches and tools for security in software and hardware development and assessment

HORIZON-CL3-2026-02-CS-ECCC-02 (IA)

EUR 21 200 000

Enhancing the Security, Privacy and Robustness of AI Models and Systems (SecureAI)

HORIZON-CL3-2026-02-CS-ECCC-03 (RIA)

EUR 15 000 000

Advanced cryptographic schemes and High-Assurance high-speed cryptographic implementations

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON-CL3-2026-02-CS-ECCC-01 (1/3)

Approaches and tools for security in software and hardware development and assessment

Scope

The increasing complexity and globalisation of software and hardware supply chains introduce new vulnerabilities that cyber adversaries can exploit. Ensuring the **security of both software and hardware components** across the lifecycle of digital systems is paramount. This topic aims to develop **innovative tools, methods, and processes** to secure the entire ecosystem of software and hardware development.

Proposals **should explicitly select one** main area of focus but can also address both:

a) Secured hardware systems over trusted Chips

b) Software Supply Chain security

HORIZON-CL3-2026-02-CS-ECCC-01 (2/3)

Approaches and tools for security in software and hardware development and assessment

Expected outcome

Proposals are expected to contribute to one or more of the following:

- ✓ Enhanced **security frameworks for both hardware and software supply chains,** building on root-of-trust architectures and **secure lifecycle management**;
- ✓ **Secure and trusted chip architectures** for next-generation computing and networking systems;
- ✓ **Integrated security-by-design approaches** in software development, aimed to be aligned with relevant regulatory requirements;
- ✓ **Security testing methodologies**, including formal verification approaches and AI-driven security testing methodologies;
- ✓ Standardized methodologies for **hardware security assessment**, also contributing to cybersecurity certification.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON-CL3-2026-02-CS-ECCC-01 (3/3)

Type of Action:	Research and Innovation Actions (RIA)
Grant amount:	EUR 3-4 million

Indicative number of projects to be funded: 4-5

Targeted stakeholders:	General requirements apply (as described in General Annex B)

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON-CL3-2026-02-CS-ECCC-02 (1/3)

Enhancing the Security, Privacy and Robustness of AI Models and Systems (SecureAI)

Scope

The increasing reliance on AI in cybersecurity, critical infrastructure, and decision-making processes raises concerns about the security and robustness of AI systems. This topic **aims to strengthen the resilience of AI systems and algorithms** against various threats and attacks, such as enhancing their resilience against adversarial attacks, backdoor injections, and data poisoning.

Proposals should develop **real-time anomaly detection, mitigation techniques** to defend against adversarial attacks and **robust federated learning techniques**, in synergies with leading efforts on AI transparency, and in compliance with the AI Act.

HORIZON-CL3-2026-02-CS-ECCC-02 (2/3)

Enhancing the Security, Privacy and Robustness of AI Models and Systems (SecureAI)

Expected outcome

Proposals are expected to contribute to one or more of the following:

- ✓ **Robust AI models and systems** capable of resisting different classes of adversarial manipulation;
- ✓ **Innovative defence mechanisms for AI** models and systems against new attack families;
- ✓ Methodologies for **detecting and mitigating attacks**, such as data poisoning, backdoor exploitation and misclassification;
- ✓ AI systems leveraging **privacy-enhancing technologies** that maintain data confidentiality and regulatory compliance, enabling trusted in-house AI deployments (e.g., for governments and enterprises).

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON-CL3-2026-02-CS-ECCC-02 (3/3)

Type of Action: Innovation Actions (IA)

Grant amount: EUR 3-4 million

Indicative number of projects to be funded: 4-5

Targeted stakeholders: General requirements apply (as described in General Annex B)

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON-CL3-2026-02-CS-ECCC-03 (1/4)

Advanced cryptographic schemes and High-Assurance high-speed cryptographic implementations

Scope

The development of **new digital signatures and advanced cryptographic schemes**, tailored specifically to the use cases and requirements in the context of wallets/eIDs, for privacy and business applications.

Another key area is the development of **High-Assurance Cryptographic Software** (HACS), including automated evaluation methods.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON-CL3-2026-02-CS-ECCC-03 (2/4)

Advanced cryptographic schemes and High-Assurance high-speed cryptographic implementations

Technology Areas to be Addressed

Proposals should address one of the following technology areas:

Design and implementation of **PQC advanced schemeds and protocols** for enhanced security and privacy, also including schemes other than lattice-based approaches if relevant. Proposals should also include recommendations that balance security, performance, and usability in practical applications and be based on o pen-source reusable software libraries.

Development of a **unified specification language to formalise and document conditions on cryptographic safety and security** in software implementations; development and improvement of tools and methodologies that can be used to evaluate both the implementation and the usage of cryptography in software applications and provide formal machine-checked guarantees of correctness and security. Proposals should also consider improving existing HACS tools and their integration in such software implementations.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON-CL3-2026-02-CS-ECCC-03 (3/4)

Advanced cryptographic schemes and High-Assurance high-speed cryptographic implementations

Expected outcome

Proposals are expected to contribute to one or more of the following:

- ✓ **Formal verification tools, improved High-Assurance Cryptographic Software (HACS) approaches** and their integration in software workflows, to provide **strong security guarantees in post-quantum migration**, and enable streamlined evidence-based evaluation of secure systems that use cryptography;
- ✓ **Quantum-resistant cryptographic primitives**, also other than lattice-based approaches if relevant, that **enhance the security and privacy of digital wallets, both for natural persons and wallets**, as well as the design and implementation of post-quantum solutions for entity authentication and authenticated key establishment over insecure networks.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON-CL3-2026-02-CS-ECCC-03 (4/4)

Type of Action: Research and Innovation Actions (RIA)

Grant amount: EUR 2-3 million

Indicative number of projects to be funded: 3-4

Targeted stakeholders: General requirements apply (as described in General Annex B)

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON-CL3-2026-02-CS-ECCC

Specific call conditions

Eligibility Conditions

In order to achieve the expected outcomes, and safeguard the Union's strategic assets, interests, autonomy, and security, participation in this topic is limited to legal entities established in **Member States and Associated Countries.**

In order to guarantee the protection of the strategic interests of the Union and its Member States, 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.

Financial Set-up

Eligible costs will take the form of a **Lump-Sum.**

Security Sensitive Topic

Some activities resulting from this topic may involve using classified background and/or producing of security sensitive results (EUCI and SEN).

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

HORIZON-CL3-2026-02-CS-ECCC

References

- Horizon Europe Worl Programme 2026-2027 - 6. Civil Security for Society
  - HORIZON-CL3-2026-02-CS-ECCC Call

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