Horizon Europe cluster 3 Civil Security for Society

Horizon Work Programme 2025 – Increased Cybersecurity Topics (CS)

Destination – Increased Cybersecurity 1/2

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) to ensure their robustness and continuity in the face of severe disruptions;

Destination – Increased Cybersecurity 2/2

- Encourage the development of the European Cybersecurity Competence Community, in close collaboration with the European Cybersecurity Competence Centre (ECCC) to avoid duplication;
- Particular attention will be given to SMEs, who play a crucial role in the cybersecurity ecosystem and in overall EU digital single market competitiveness, by promoting security and privacy ‘by design’ in existing and emerging technologies

Overview of HE CL3 CS 2025 call

Topic	Instrument	EUR (million)	Projects	Opening date	Deadline date
HORIZON-CL3-2025-02-CS-ECCC-01: Generative AI for Cybersecurity applications	RIA	40.00	Up to 3 projects	12 June 2025	12 November 2025
HORIZON-CL3-2025-02-CS-ECCC-02: New advanced tools and processes for Operational Cybersecurity	IA	23.55	Up to 4 projects	12 June 2025	12 November 2025
HORIZON-CL3-2025-02-CS-ECCC-03: Privacy Enhancing Technologies	RIA	11.00	Up to 3 projects	12 June 2025	12 November 2025
HORIZON-CL3-2025-02-CS-ECCC-04: Security evaluations of Post-Quantum Cryptography (PQC) primitives	RIA	4.00	Up to 2 projects	12 June 2025	12 November 2025
HORIZON-CL3-2025-02-CS-ECCC-05: Security of implementations of PostQuantum Cryptography algorithms	RIA	6.00	Up to 2 projects	12 June 2025	12 November 2025
HORIZON-CL3-2025-02-CS-ECCC-06: Integration of Post-Quantum Cryptography (PQC) algorithms into high-level protocols	RIA	6.00	Up to 2 projects	12 June 2025	12 November 2025

Topic 01: Generative AI for Cybersecurity applications

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.

   i. Advanced threat and anomaly detection and analysis

   ii. Adaptive security measures

   iii. Enhanced authentication and access control

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.

   i. Application of the national and EU regulation in digital systems

   ii. Adaptation to a dynamic environment

Topic 02: New advanced tools and processes for Operational Cybersecurity

Proposals should address **at least two** 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

Topic 03: Privacy Enhancing Technologies (1/2)

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

Topic 03: Privacy Enhancing Technologies (2/2)

- 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.

Topic 04: Security evaluations of Post-Quantum Cryptography (PQC) primitives

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;
- 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.

Topic 05: Security of implementations of Post-Quantum Cryptography algorithms

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

Topic 06: Integration of Post-Quantum Cryptography (PQC) algorithms into high-level protocols

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

Important INFO - Difference from previous WPs:

The topics are at the end of the text under Appendix 3 of the Horizon Europe Work Programme 2025

European Commission

Thank you

European Commission