EU CYBERSECURITY STRATEGY

Policy briefing

Weblink	https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy
Relevance	☐ National policy X EU policy ☐ other: _____
Briefing done by	Melina Di Matteo

Short summary of the policy

The European Union has progressively developed initiatives to strengthen cybersecurity and protect its digital ecosystem. Key milestones include the creation of ENISA (2004), the first European cybersecurity strategy "An open, safe and secure cyberspace" (2013), the NIS Directive (2016), the Cyber Diplomacy Toolbox (2017), and the Cybersecurity Act (2019), which gave ENISA a permanent mandate and established a European cybersecurity certification framework.

With the rise of sophisticated cyber threats and vulnerabilities in critical sectors, the EU recognized the need for a unified approach to resilience. In December 2020, the European Commission presented the new European Cybersecurity Strategy, adopted by the European Council and Parliament in 2021, aiming to create a secure and reliable digital environment for citizens, businesses, and public administrations by 2030.

The strategy emphasizes integrating cybersecurity throughout the digital transition, strengthening operational capabilities, and establishing mechanisms such as the Joint Cybersecurity Unit and the European Cyber Shield, a network of security operations centers for continuous monitoring and rapid response. It also promotes international cooperation based on European values, updates the NIS Directive (NIS2) to cover additional sectors with stricter enforcement, and addresses the shortage of skilled cybersecurity professionals through education, training, and awareness-raising campaigns.

Main objectives of the policy

- Strengthen EU cybersecurity resilience and capacities.
- Protect critical infrastructure and essential services (e.g., NIS2).
- Support innovation and advanced cybersecurity technologies.
- Foster international cooperation for a secure cyberspace.
- Promote coordination among Member States, industry, and EU institutions for incident response.
- Develop cybersecurity skills, awareness, and education.
- Embed cybersecurity across the digital transition, including AI, quantum, and 5G.
- Improve EU-wide cyber crisis management and large-scale incident response.
- Secure ICT supply chains by enforcing high-security standards.

The DEP4ALL project is funded by the European Commission under the Digital Europe Programme, under grant agreement no. 101167919. Any opinions expressed in these pages are those of the author/organisation and do not necessarily reflect the views of the European Commission.

Context and relation to the Digital Europe Programme (DEP)

In general, DEP contributes to this Strategy by funding projects that strengthen digital resilience, support innovation in cybersecurity and promote cooperation between Member States:

EU Cybersecurity Strategy	DEP
European Cyber Shield	Development and enhancement of SOCs, enabling continuous monitoring and rapid response to cyber-attacks on a European scale.
Cybersecurity training and awareness	Training and retraining programs to bridge the cybersecurity skills gap, as well as awareness campaigns.
EU legislation	Support of organisations to comply with the directives enhanced cybersecurity requirements (e.g. NIS2, Cyber Solidarity Act).
Collective response to cyber crises	Initiatives to improve the collective response to cyber incidents on a European scale, notably through coordination between member states, businesses and European institutions.
Safe and resilient digital transformation	Initiatives to ensure the EU's digital transformation is carried out securely, while building resilience to cyber threats.
Technological innovation and research	Supports the funding of advanced cybersecurity technologies (e.g. based on AI, machine learning, and other innovative technologies).
Securing critical infrastructure	Supports projects designed to ensure the security of critical infrastructure and digital services as part of the digital transformation.
Cybersecurity for SMEs	Solutions, training programs, and awareness initiatives to strengthen the cybersecurity of SMEs, while encouraging their involvement in DEP projects.

Parts of the policy directly related to specific objectives (SO) in DEP

SO	Policy relevance	DEP calls
SO1: High Performance Computing	Supports cryptography for future quantum threats and supercomputing for threat simulation.	Provide HPC access to advance cybersecurity innovation, threat detection, and resilience.
SO2: AI Continent	Enables secure data sharing and AI-powered threat detection across sectors.	Develop secure, interoperable data spaces and AI tools to detect and mitigate cyber threats.
SO3: Cybersecurity	Builds a European network of SOCs, promotes trusted technologies, and fosters cross-border collaboration.	Support SOCs, certified solutions, and frameworks for threat intelligence sharing in line with NIS2.
SO4: Advanced Digital Skills	Addresses the shortage of cybersecurity professionals via education, training, and certification	Fund innovative training programs and academia-industry partnerships to close the skills gap
SO5: Deployment and Best Use of Digital Capacities	Promotes accessible, scalable cybersecurity solutions for SMEs and public organizations.	Support adoption of practical cybersecurity solutions to secure digital transformation.
SO6: Semiconductors	Strengthens the EU semiconductor ecosystem for technological sovereignty, supply chain security, and infrastructure resilience.	Fund secure semiconductor-based technologies, PQC deployment, Cyber Hub migration, and SME cybersecurity solutions.

The DEP4ALL project is funded by the European Commission under the Digital Europe Programme, under grant agreement no. 101167919. Any opinions expressed in these pages are those of the author/organisation and do not necessarily reflect the views of the European Commission.

Activities in the DEP Work Programme 2025-27 contributing to the objectives of the policy

1) Cyber Hubs and Cross-Border Cooperation

DEP topics:

- National Cyber Hubs *(2026, call for expression of interest)*
- Cross-Border Cyber Hubs *(2027, call for expression of interest)*
- Strengthening the Cyber Hubs ecosystem and enhancing information sharing *(2026 [EUR 20 million] and 2027 [EUR 12 million], simple grant)*

Policy relevance: The EU Cybersecurity Strategy emphasizes creating a European network of Security Operations Centres and Cyber Hubs to enhance real-time threat detection, cross-border cooperation, and incident response.

DEP support: These calls fund the creation, expansion, and interoperability of national and cross-border Cyber Hubs, strengthening operational capabilities, enabling threat intelligence sharing, and supporting coordinated responses to cyber incidents in line with the Strategy.

2) Preparedness and Mutual Assistance

DEP topics:

- Coordinated preparedness testing and other preparedness actions *(2026 [EUR 5 million] and 2027 [EUR 15 million], simple grant)*
- Mutual assistance *(2026 [EUR 2 million] and 2027 [EUR 2 million], grant for named beneficiaries)*
- Enhancing the NCC network *(2026, Simple grant, EUR 46 million)*

Policy relevance: The Strategy highlights the need for EU-wide crisis management frameworks, rapid response mechanisms, and coordinated assistance among Member States during major cyber incidents.

DEP support: Calls support joint exercises, technical assistance, and network strengthening, improving crisis readiness, cross-border coordination, and rapid mutual support during large-scale incidents.

3) AI and Advanced Cybersecurity Solutions

DEP topics:

- Cybersecure tools, technologies and services relying on AI *(2026 [EUR 15 million] and 2025 [EUR 15 million], simple grant)*
- Strengthening cybersecurity capacities of European SMEs with cybersecure AI-powered solutions *(2026 [EUR 20 million] and 2027 [EUR 12 million], simple grant)*
- Uptake of innovative cybersecurity solutions for SMEs *(2026 [EUR 15 million] and 2025 [EUR 15 million], SME support action)*

Policy relevance: The Strategy promotes innovation in cybersecurity, including AI-based threat detection and secure technologies for SMEs, to ensure a trusted digital economy and resilience against emerging threats.

DEP support: These calls fund AI-driven cybersecurity tools, secure SME adoption of advanced solutions, and support research and deployment of technologies aligned with the EU's operational and innovation objectives.

4) Post-Quantum Cryptography

DEP topic: Migration of Cyber Hubs to PQC *(2027, EUR 7 million, simple grant)*

Policy relevance: The Strategy highlights preparing for future cyber threats, including quantum computing risks that could compromise cryptography protecting critical infrastructure.

DEP support: These calls provide funding for PQC infrastructure, secure migration of Cyber Hubs, and testing environments, ensuring Europe's cryptographic resilience and long-term security of critical digital services.

The DEP4ALL project is funded by the European Commission under the Digital Europe Programme, under grant agreement no. 101167919. Any opinions expressed in these pages are those of the author/organisation and do not necessarily reflect the views of the European Commission.

5) Regulatory Compliance and Capacity Building

DEP topic: Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements *(2026 [EUR 20 million] and 2027 [EUR 12 million], simple grant)*

Policy relevance: Supports the EU Cybersecurity Strategy by ensuring compliance with NIS2 and the Cybersecurity Act, strengthening EU-wide resilience.

DEP support: Funds projects that enhance capacities, tools, and processes to meet regulatory requirements and improve coordinated cybersecurity across Member States.

Related policies and further information

For related events, please check out the online calendars: Shaping Europe's digital future, ECCC

General information on the EU cybersecurity policies: EU cybersecurity policies

Related policies:

- Directive (EU) 2022/2555 – NIS 2 Directive
- EU Cybersecurity Act
- Cyber Resilience Act
- EU Cybersecurity Strategy for the Digital Decade
- EU Cyber Solidarity Act

The DEP4ALL project is funded by the European Commission under the Digital Europe Programme, under grant agreement no. 101167919. Any opinions expressed in these pages are those of the author/organisation and do not necessarily reflect the views of the European Commission.