DEP4ALL
THE NCP NETWORK FOR THE DIGITAL EUROPE PROGRAMME

Funded by the European Union

EU Cybersecurity Strategy

Policy brief

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 gradually adopted several initiatives to strengthen cybersecurity and protect its digital ecosystem. These include among others: the creation of ENISA, which provides expertise and support to member states and European institutions (2004); the first European cybersecurity strategy entitled "An open, safe and secure cyberspace" (2013); the NIS Directive, on the security of networks and information systems (2016) ; the Cyber Diplomacy Toolbox, aimed at strengthening EU resilience via diplomatic measures (2017); or the Cybersecurity Act, which gave ENISA a permanent mandate and established a framework for cybersecurity certification schemes at European level (2019).

However, as society transforms digitally, new forms of threat have emerged, including increasingly sophisticated and large-scale attacks (e.g. ransomware attacks or intrusions into critical infrastructure). It has revealed vulnerabilities in key sectors. The need for a unified and innovative European approach to strengthen resilience in the face of these growing risks has been highlighted.

As part of the Digital Decade, the European Commission presented a new European Cybersecurity Strategy in December 2020. This strategy aims to build a powerful and resilient digital Europe by 2030. It has been adopted by the European Council and Parliament in 2021, which aims to create a secure and reliable digital environment for EU citizens, businesses and public administrations. The strategy underlines the importance of integrating cybersecurity into every stage of the digital transition, considering resilience and security as essential elements for a successful transformation.

A key focus of this initiative is the strengthening of operational capabilities to better prevent, detect and respond to cyber threats. Among the flagship measures is the proposal to create a Joint Cybersecurity Unit, a mechanism designed to strengthen coordination between member states and European institutions in the management of major crises. In addition, the creation of a European Cyber Shield, comprising a network of security operations centers across Europe, to continuous monitoring and rapid response to attacks.

Faced with the transnational nature of cyberthreats, the EU is committed to strengthening its partnerships with global players and international organizations, aiming to establish a stable and secure cyberspace, founded on European values of democracy and respect for the rule of law.

On the legislative front, there is the revision of the NIS Directive (NIS2). This update extends the scope of the directive to new critical sectors and introduces dissuasive sanctions for entities failing to comply with security obligations.

Another major challenge is the shortage of cybersecurity skills. The strategy includes concrete actions to develop a skilled workforce, by supporting education and continuing training programs tailored to market needs. At the same time, awareness-raising campaigns aim to better inform citizens about good cybersecurity practices, so that they can navigate the digital space more safely.

Main objectives of the policy (in bullet points)

- Strengthen cybersecurity resilience and capacity across the EU.
- Protect critical infrastructure and essential services through enhanced regulations (eg: NIS2 Directive).
- Support cybersecurity innovation and the development of advanced technologies.
- Foster international partnerships to promote a secure and stable global cyberspace.
- Encourage cooperation among Member States, industry, and EU institutions for cybersecurity incident response and preparedness.
- Develop cybersecurity skills and awareness through targeted initiatives.
- Promote a cyber-secure digital economy by embedding cybersecurity into the digital transition, including in emerging technologies like AI, quantum computing, and 5G.
- Develop a common cyber crisis management framework to improve the EU's ability to handle large-scale cyber incidents through better coordination mechanisms.
- Strengthen the cybersecurity of supply chains by ensuring ICT products, software, and hardware meet high-security standards to mitigate supply chain risks.

Context and relation to DIGITAL EUROPE

In general, DEP contributes to the European Cybersecurity 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	Funds projects for the development and enhancement of SOCs, enabling continuous monitoring and rapid response to cyber-attacks on a European scale.
Cybersecurity training and awareness	Funds training and retraining programs to bridge the cybersecurity skills gap, as well as awareness campaigns.
EU legislation	Funds projects that help organisations to comply with the directives enhanced cybersecurity requirements (e.g. NIS2, Cyber Solidarity Act).
Collective response to cyber crises	Supports initiatives that 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	Supports initiatives that ensure the EU's digital transformation is carried out securely, while building resilience to cyber threats.
Technological innovation and research (foster innovation in cybersecurity to address emerging threats)	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	Funds solutions, training programs, and awareness initiatives to strengthen the cybersecurity of SMEs, while encouraging their active involvement in DEP projects.

What parts of the Policy are directly related to specific objectives (SO) in DEP

SO1: High Performance Computing (HPC)

Relevant sections of the policy:

- Supporting the development of cryptographic methods to protect critical infrastructure against future quantum threats.
- Leveraging supercomputing for predictive analytics and simulation of cyber threats.

DEP calls supporting cybersecurity in supercomputing:

- DEP funding opportunities for supercomputing access provide tools to advance cybersecurity innovation (e.g. strengthening threat detection and overall resilience).
- Initiatives leveraging supercomputing for developing cryptographic solutions, conducting advanced threat analysis, or simulating cyber incidents can capitalize on these resources to meet strategic objectives.

SO2: Artificial Intelligence (AI)

Relevant sections of the policy:

- Supports the creation of secure data-sharing frameworks, ensuring interoperability and resilience across sectors.
- Highlights the potential of AI tools to automate threat detection and response, reinforcing the EU's cyber defense capabilities

DEP calls supporting cybersecurity in AI, data, and cloud:

- DEP calls emphasize the development of secure and interoperable data spaces, which align with the strategy's goal of protecting sensitive information across EU-wide sectors.
- Projects that integrate AI to detect and mitigate threats or secure federated cloud infrastructures are important to fulfilling these policy priorities

SO3: Cybersecurity

Relevant sections of the policy:

- The European Cybersecurity Strategy emphasizes creating a European network of SOCs to provide real-time threat detection and response capabilities across borders.
- The strategy prioritizes ensuring that critical sectors adopt trusted and certified cybersecurity technologies.
- Another objective of the strategy is to facilitate collaboration and information sharing between Member States to combat transnational cyber threats.

DEP calls supporting cybersecurity:

- DEP calls for cybersecurity directly aligns with the European Cybersecurity Strategy's objectives. These calls can focus on developing advanced cross-border SOCs to enable real-time monitoring and enhance cooperation across Member States. DEP calls are also contributing to the adoption of certified and interoperable cybersecurity solutions, supporting the strategy's goal to secure critical infrastructure. Additionally, other calls emphasize the creation of frameworks for sharing cyber threat intelligence or ensuring compliance with EU legislation (e.g. NIS2).

SO4: Advanced Digital Skills

Relevant sections of the policy:

- Identifying the urgent need to address the EU's shortage of skilled cybersecurity professionals through targeted education and training programs.

- Promoting EU-wide certification standards for cybersecurity training to ensure consistency and trust in skills development.

DEP calls supporting skills development in cybersecurity:

- DEP calls encourage the creation of innovative training programs and partnerships between academia and industry, aligning with the strategy's goal of addressing the skills gap.

SO5: Deployment and Best Use of Digital Capacities and Interoperability

Relevant sections of the policy:

- The strategy promotes accessible and scalable cybersecurity solutions for SMEs and public organizations as part of the broader goal of securing digital transformation.
- Encouraging the use of emerging technologies to secure transactions and enhance public service delivery.

DEP Calls Supporting Skills Development in Cybersecurity:

- DEP calls aim to help SMEs and public organizations adopt cybersecurity solutions that are practical and adapted to their specific needs, perfectly aligning with the priorities outlined in the strategy.

Which activities in the current DEP Work Programme contribute to meeting the objectives of the policy

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC: National SOCs

- Deadline: 27-03-25
- Description: aims to strengthen the capacities of existing or new national SOCs. Activities may include acquiring equipment, tools, and data flows, as well as training cybersecurity analysts. The goal is to create world-class SOCs in the EU, leveraging advanced technologies like AI to improve threat intelligence and foster cross-border cooperation through interconnected SOC platforms.

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCPLAT: Enlarging existing or Launching New Cross-Border SOC Platforms

- Deadline: 27-03-25
- Description: focuses on creating or enhancing cross-border SOC platforms, where national SOCs collaborate to improve cybersecurity threat analysis, detection, and prevention across EU member states. The aim is to enable cross-border sharing of information and resources, enhancing collective cybersecurity capabilities across the EU.

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCSYS: Strengthening the SOC Ecosystem

- Deadline: 27-03-25
- Description: seeks to develop and deploy advanced cybersecurity systems and tools based on enabling technologies such as AI to enhance the detection, analysis, and prevention of cyber threats.

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH: Development and Deployment of Advanced Key Technologies

- Deadline: 27-03-25

- Description: focuses on developing and deploying advanced cybersecurity technologies to enhance the EU's capabilities in detecting and responding to cyber threats. The goal is to integrate key digital technologies (AI, big data analytics, quantum computing, etc.) into the cybersecurity infrastructure to improve efficiency, scalability, and data sharing capabilities, ensuring the security of critical infrastructure and services across the EU.

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER: Preparedness Support and Mutual Assistance, Targeting Larger Industrial Operations and Installations

- Deadline: 27-03-25
- Description: provides support to large industrial operations and essential service providers, focusing on improving cybersecurity preparedness. The aim is to improve the cybersecurity posture of critical infrastructure by providing tailored support in evaluating and mitigating cyber risks, creating test environments, and deploying tools to ensure effective protection against cyber threats.

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-CYBERSEC-02: Support for Implementation of EU Legislation on Cybersecurity and National Cybersecurity Strategies (2024)

- Deadline: 27-03-25
- Description: This call supports the strengthening of technical, operational, and strategic cybersecurity cooperation at the EU level. It aims to help member states implement the NIS2 Directive, Cybersecurity Act, and other related regulations.

Please match any specific activity mentioned in the policy with concrete call topics from the current/upcoming DEP Work Programme

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOC: aligns with the EU Cybersecurity Strategy's goal of enhancing the resilience of Member States' cybersecurity infrastructures by reinforcing national SOCs to improve their cyber defense capabilities.

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-SOCPLAT: supports the EU Cybersecurity Strategy's objective of fostering cross-border cooperation and collaboration in cybersecurity, by developing platforms for sharing threat intelligence across Member States.

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH: contributes to the EU Cybersecurity Strategy’s focus on advancing cybersecurity technologies, particularly AI and data analytics, to strengthen cybersecurity defenses against evolving threats.

DIGITAL-ECCC-2024-DEPLOY-CYBER-07-LARGEOPER: supports the EU Cybersecurity Strategy's priority of enhancing the protection of critical infrastructure and key services from cyber threats through vulnerability testing and preparedness exercises

Events

For finding related events, please check out the following online calenders: Shaping Europe’s digital future, ECCC