ECCC

EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

ECCC DEP Work Programme: A Three-Year Investment Plan for Improving Cybersecurity

Polyvios Hadjiyiangou, Head of Operations

Second national
NCC-HR conference

Overview

- **Strategic Priorities:** EU cybersecurity goals and policy context
- **From Vision to Deployment:** Operational shift under DEP 2025–2027 and ECCC's leadership
- **Key Actions and Topics Overview:**
  - ✓ New technologies, AI and post-quantum transition
  - ✓ Cyber Solidarity Act Implementation
  - ✓ Additional actions improving EU cyber resilience

Strategic Rationale and Vision

- EU aims to reinforce its technological sovereignty in cybersecurity and reduce strategic dependencies.
- The Cybersecurity Strategy for the Digital Decade sets the foundation:
  - ✓ **securing critical infrastructure (e.g. 5G),**
  - ✓ **safeguarding European digital assets, and**
  - ✓ **promoting trust.**
- Cybersecurity is not only a technical goal, but a cornerstone of the EU Security Union Strategy.
- The Digital Europe Programme (DEP) is the financial and policy engine to transform this vision into concrete, operational outcomes.

ECCC is translating EU strategy into deployment-driven impact ensuring that R&D in cybersecurity leads to real capabilities across Member States.

Deployment – a new operational era

Moving Beyond Research: Co-Investment for Operational Readiness

- As of 2025, the ECCC leads the DEP WP for Cybersecurity, marking a shift to deployment at scale.
- The ECCC is now fully responsible for the drafting and implementation, reinforcing its leadership in building trusted, sovereign cybersecurity infrastructures across the Union.
- Specific Objective 3 of DEP (“Cybersecurity and Trust”) now directly supports:
  - ✓ **Rolling out validated solutions**
  - ✓ **Operationalising tools and infrastructure**
  - ✓ **Scaling capabilities in line with regulatory needs (NIS 2, CRA, Cyber Solidarity Act)**

Evolving policy landscape – legislative foundations

A Stronger Legal Backbone for EU Cybersecurity Deployment

The ECCC DEP Work Programme 2025–2027 operates within a fast-moving EU cybersecurity landscape shaped by:

- **NIS 2 Directive**: Broader scope, stricter obligations, harmonised supervision; transposition
- **Cyber Resilience Act (CRA):** Lifecycle cybersecurity obligations for digital products and services;
- **Cyber Solidarity Act (CSoA):** New legal tool for joint preparedness, situational awareness, mutual assistance

- The ECCC is tasked with **implementing major CSoA provisions**, including:

✓ Mapping EU-wide cyber capabilities

✓ Coordinating grant funding for Cyber Hubs and preparedness testing

✓ Supporting incident response and mutual assistance across Member States

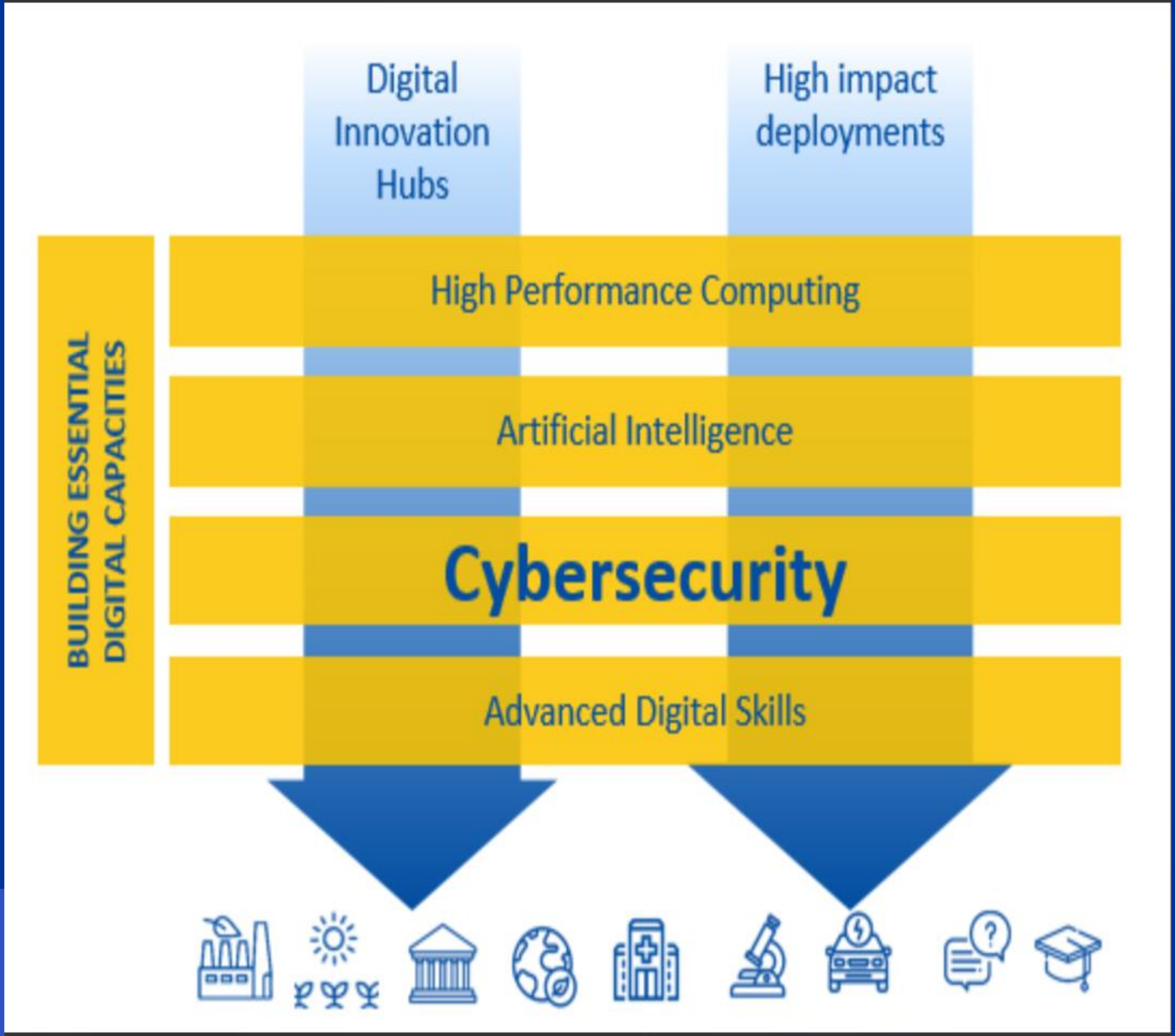
Aligning with Broader EU Cybersecurity and Political Priorities

ECCC DEP WP aligns with:

- The **EU Security Union Strategy**, recognising cybersecurity as foundational to EU sovereignty.
- The **Political Guidelines 2024–2029**, including focus on healthcare cyber resilience and submarine cable security.
- **Cybersecurity Act (CSA)**, which provides the basis for EU-wide certification schemes (EUCC, EUCS, EU5G).

ECCC ensures funded solutions align with policy goals and are designed to comply with certification schemes

DEP Objectives – Empowering Europe’s Digital Leadership



ECCC Role:

- Operate under DEP Objective 3 Cybersecurity.
- Translates strategic goals into action by coordinating funding, shaping calls for proposals, and supporting adoption across Member States.

Topics and budget are subject to change

	Areas and topics	2025	2026	2027
	New technologies. AI & to post-quantum transition Area 1			
2.1	Cybersecure tools, technologies and services relying on AI	x	x	x
2.2	Strengthening cybersecurity capacities of European SMEs with cybersecure AI powered solutions		x	
2.3	Deployment of a European testing infrastructure for the transition to PQC in different usage domains	x		
2.4	Transition to post-quantum Public Key Infrastructures	x		
2.5	Migration of Cyber-Hubs to PQC			x
2.6	Uptake of innovative cybersecurity solutions for SMEs	x		x
	Cyber Solidarity Act Implementation Area 2			
2.7	National Cyber Hubs	x	x	
2.8	Cross-Border Cyber Hubs	x		x
2.9	Strengthening the Cyber Hubs ecosystem and enhancing information sharing		x	
2.10	Coordinated preparedness testing and other preparedness actions	x	x	X
2.11	Mutual assistance		x	x
	Additional actions improving EU cyber resilience Area 3			
2.12	Enhancing the NCC Network	x	x	X
2.13	Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements		X	x
2.14	Dedicated action to reinforcing hospitals and healthcare providers	x		
2.15	Dual use technologies		X	

Budget Overview

Total: €390 million over 3 years

- €142M: AI & PQC
- €121M: Cyber Solidarity
- €118M: Resilience
- €9M: Support actions

Topics and budget are subject to change	Areas and topics	2025	2026	2027
	New technologies. AI & to post-quantum transition			
2.1	Cybersecure tools, technologies and services relying on AI	x	x	x
2.2	Strengthening cybersecurity capacities of European SMEs with cybersecure AI powered solutions		x	
2.3	Deployment of a European testing infrastructure for the transition to PQC in different usage domains	x		
2.4	Transition to post-quantum Public Key Infrastructures	x		
2.5	Migration of Cyber-Hubs to PQC			x
2.6	Uptake of innovative cybersecurity solutions for SMEs	x		x
	Cyber Solidarity Act Implementation			
2.7	National Cyber Hubs	x	x	
2.8	Cross-Border Cyber Hubs	x		x
2.9	Strengthening the Cyber Hubs ecosystem and enhancing information sharing		x	
2.10	Coordinated preparedness testing and other preparedness actions	x	x	X
2.11	Mutual assistance		x	x
	Additional actions improving EU cyber resilience			
2.12	Enhancing the NCC Network	x	x	X
2.13	Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements		X	x
2.14	Dedicated action to reinforcing hospitals and healthcare providers	x		
2.15	Dual use technologies		X	

Area 1: New technologies, AI & post-quantum transition

AI for Cybersecurity and Trustworthy Deployment

- Support the development and deployment of AI and GenAI tools for cybersecurity threat detection, incident analysis, and response automation across public and private sectors.
- Enable Cyber Hubs, CSIRTs, and national authorities to leverage scalable AI technologies for Cyber Threat Intelligence (CTI) and vulnerability monitoring.
- Strengthen the security and trustworthiness of AI systems used in cybersecurity, addressing robustness, resilience, and regulatory compliance
- Promote AI systems that are secure-by-design, transparent, and aligned with the EU’s emerging AI and cybersecurity certification frameworks

ECCC funds and coordinates real-world AI deployments and
ensures security is integrated throughout the AI lifecycle—from design to operational use.

New technologies, AI & post-quantum transition

Transitioning to Post-Quantum Cryptography

Building EU Readiness for Quantum-Resilient Infrastructure

- Establish and expand European testing infrastructure for Post-Quantum Cryptography (PQC) across sectors and applications
- Support deployment of quantum-safe PKI, VPN, TLS, and digital signature schemes within Cyber Hubs and national infrastructure
- Accelerate the migration of EU cybersecurity services and software to crypto-agile, PQC-ready environments
- Raise awareness and provide tools for secure key management, hybrid cryptographic implementation, and PQC certification-readiness

ECCC drives the transition to PQC through funding, infrastructure deployment, and cross-border coordination with Member States

New technologies, AI & post-quantum transition

Supporting SMEs and Scaling Trusted Cyber Solutions

Strengthening Compliance, Market Access, and Operational Resilience

- Provide cybersecurity toolkits and services for SMEs
  - ✓ including risk assessment, threat detection, incident reporting, and compliance support with CRA, NIS 2, and EUCS
- Support development of secure-by-design software components and tools to assist SMEs in meeting legal and technical cybersecurity requirements
- Promote market-ready, high-TRL cybersecurity solutions, especially those offering EU-origin alternatives to foreign technologies

ECCC ensures SMEs and solution providers receive support to scale, comply, and secure Europe’s digital ecosystem.

Topics and budget are subject to change	Areas and topics	2025	2026	2027
	New technologies. AI & to post-quantum transition			
2.1	Cybersecure tools, technologies and services relying on AI	x	x	x
2.2	Strengthening cybersecurity capacities of European SMEs with cybersecure AI powered solutions		x	
2.3	Deployment of a European testing infrastructure for the transition to PQC in different usage domains	x		
2.4	Transition to post-quantum Public Key Infrastructures	x		
2.5	Migration of Cyber-Hubs to PQC			x
2.6	Uptake of innovative cybersecurity solutions for SMEs	x		x
	Cyber Solidarity Act Implementation			
2.7	National Cyber Hubs	x	x	
2.8	Cross-Border Cyber Hubs	x		x
2.9	Strengthening the Cyber Hubs ecosystem and enhancing information sharing		x	
2.10	Coordinated preparedness testing and other preparedness actions	x	x	X
2.11	Mutual assistance		x	x
	Additional actions improving EU cyber resilience			
2.12	Enhancing the NCC Network	x	x	X
2.13	Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements		X	x
2.14	Dedicated action to reinforcing hospitals and healthcare providers	x		
2.15	Dual use technologies		X	

Cyber Solidarity Act Implementation

National and Cross-Border Cyber Hubs

Strengthening Cyber Infrastructure for Early Warning and Threat Intelligence

- Support the creation or enhancement of National Cyber Hubs with advanced tools for real-time threat detection, CTI analysis, and coordination with CSIRTs and ISACs
- Deploy Cross-Border Cyber Hubs to share operational threat intelligence across Member States
- Activities may include monitoring submarine cables, enhancing situational awareness, and scaling automated information-sharing platforms.

ECCC leads implementation of both National and Cross-Border Cyber Hubs, managing joint procurement and complementary grants

Cyber Solidarity Act Implementation

Consolidating the Cyber Hubs Ecosystem

Integration, Information Sharing, and Public-Private Collaboration

- Support collaboration among Cyber Hubs, linking them with industry players and facilitating the adoption of AI and post-quantum technologies developed under earlier topics
- Promote technical coordination, knowledge exchange, and joint training (e.g. ECSF-based training and Capture the Flag competitions).
- Foster standardised methods for information exchange, incident notifications, and Operational Technology (OT) threat response.

The ECCC ensures consistent architecture, cooperation models, and ecosystem integration between Cyber Hubs, SOCs, and national stakeholders

Cyber Solidarity Act Implementation

Preparedness and Mutual Assistance Mechanisms

Testing, Readiness and Emergency Support at EU Scale

- Fund preparedness testing actions for critical infrastructure, supply chain defence, and scenario-based threat simulations
- Implement the Mutual Assistance Mechanism, providing technical support during large-scale incidents via trusted public-sector responders
- Preparedness actions may draw on collaboration with EU satellite systems, sea-based sensors, and situational analysis tools.

ECCC supports preparedness and mutual assistance actions under the Cyber Solidarity Act, coordinating financial instruments and operational support across Member States

Topics and budget are subject to change	Areas and topics	2025	2026	2027
	New technologies. AI & to post-quantum transition			
2.1	Cybersecure tools, technologies and services relying on AI	x	x	x
2.2	Strengthening cybersecurity capacities of European SMEs with cybersecure AI powered solutions		x	
2.3	Deployment of a European testing infrastructure for the transition to PQC in different usage domains	x		
2.4	Transition to post-quantum Public Key Infrastructures	x		
2.5	Migration of Cyber-Hubs to PQC			x
2.6	Uptake of innovative cybersecurity solutions for SMEs	x		x
	Cyber Solidarity Act Implementation			
2.7	National Cyber Hubs	x	x	
2.8	Cross-Border Cyber Hubs	x		x
2.9	Strengthening the Cyber Hubs ecosystem and enhancing information sharing		x	
2.10	Coordinated preparedness testing and other preparedness actions	x	x	X
2.11	Mutual assistance		x	x
	Additional actions improving EU cyber resilience			
2.12	Enhancing the NCC Network	x	x	X
2.13	Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements		X	x
2.14	Dedicated action to reinforcing hospitals and healthcare providers	x		
2.15	Dual use technologies		X	

Area 3– Strengthening EU Cyber Resilience & Compliance

Supporting National Capacity, Legislative Alignment & Healthcare Resilience

- Strengthen the **National Coordination Centres (NCCs)** to support cybersecurity ecosystems in Member States, particularly for SMEs and public authorities
- Fund actions that help organisations **comply with EU cybersecurity legislation**, including NIS 2, the Cyber Resilience Act, and the Cybersecurity Act
- **Special focus on the health sector to support the cybersecurity of hospitals and healthcare providers (Political Guidelines 2024–2029 and Action Plan on the Cybersecurity of Hospitals and Healthcare providers).**

The ECCC enables these actions through targeted funding, coordination with NCCs, and strategic oversight of capacity-building efforts and sectoral deployment prioritie

Additional actions improving EU cyber resilience

Enabling Dual-Use Innovation for Civil and Defence Needs

Trusted Cybersecurity Solutions for Strategic Infrastructure and Sovereignty

- Promote development and deployment of dual-use cybersecurity technologies, including:
  - ✓ Quantum-resistant solutions
  - ✓ AI-enabled threat analytics
  - ✓ Zero Trust Architectures
- Encourage interoperability between civil and defence applications and align innovation with both market and strategic needs.
- **Support solutions for surveillance and protection of critical undersea infrastructure, such as submarine cables.**
- Support the emergence of market-ready, EU-origin alternatives to foreign cybersecurity solutions.

The ECCC manages the selection and funding of dual-use innovation projects and fosters synergies between DEP and defence-oriented cybersecurity programmes

Follow us:

ECCC Newsletter

ECCC LinkedIn

ECCC Twitter/X

ECCC website

ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

Thank you!

ECCC

EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

ECCC - Navigating DEP Calls: What's Currently Available?

Polyvios Hadjiyiangou, Head of Operations

Second national
NCC-HR conference

Overview

- **Digital Europe Programme – DIGITAL-ECCC-2025-DEPLOY-CYBER-08**
- **Digital Europe Programme – DIGITAL-ECCC-2025-DEPLOY-CYBER-09**

✓ *Topics overview*

✓ *Awards criteria*

✓ *Budget categories and cost eligibility*

✓ *Timetable and deadlines*

Topics and budget are subject to change	Areas and topics	2025	2026	2027
	New technologies. AI & to post-quantum transition			
2.1	Cybersecure tools, technologies and services relying on AI	x	x	x
2.2	Strengthening cybersecurity capacities of European SMEs with cybersecure AI powered solutions		x	
2.3	Deployment of a European testing infrastructure for the transition to PQC in different usage domains	x		
2.4	Transition to post-quantum Public Key Infrastructures	x		
2.5	Migration of Cyber-Hubs to PQC			x
2.6	Uptake of innovative cybersecurity solutions for SMEs	x		x
	Cyber Solidarity Act Implementation			
2.7	National Cyber Hubs	x	x	
2.8	Cross-Border Cyber Hubs	x		x
2.9	Strengthening the Cyber Hubs ecosystem and enhancing information sharing		x	
2.10	Coordinated preparedness testing and other preparedness actions	x	x	X
2.11	Mutual assistance		x	x
	Additional actions improving EU cyber resilience			
2.12	Enhancing the NCC Network	x	x	X
2.13	Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements		X	x
2.14	Dedicated action to reinforcing hospitals and healthcare providers	x		
2.15	Dual use technologies		X	

DEP-08 Call topics list

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-PublicPQC

EUR 15 000 000

- **Transition to post-quantum Public Key Infrastructures**

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC

EUR 10 000 000

- **Enhancing the NCC Network**

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CyberHEALTH

EUR 30 000 000

- **Dedicated action to reinforcing hospitals and healthcare providers**

All topics are subject to the provisions of article 12(5) of the Digital Europe Programme Regulation.

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-PublicPQC

Transition to post-quantum Public Key Infrastructures

Objective:

- tackle the challenges of an effective integration of PQC algorithms in Public Key Infrastructures (PKIs), which offers efficient migration strategies and strong business continuity guarantees.

Scope:

Proposals shall target activities on the following subjects:

- Design of digital signature combiners and key encapsulation mechanism combiners.
- Testing how certificates are deployed in the protocols that use them.
- Development of new protocols for Automatic Certificate Management and revocation, and for (privacy-friendly) certificate-transparency.
- Development of methods and tools that experts can use across different PKI domains, including all parts of key management for asymmetric systems.
- Proposals should carefully consider requirements and limitations—like security level, performance and backward compatibility—across many applications in critical sectors (such as governmental services, telecom, banking, smart homes, e-Health, automotive, and others).

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-PublicPQC

- Indicative duration of the action: 36 months
- Type of Action: Simple Grants
- Grant amount: EUR 4-5 million
- Indicative number of projects to be funded: 3
- Types of beneficiaries: All actors in PKI chain

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC

Enhancing the NCC Network

Based on the financing received in previous years and on the different operational start dates in the Member States, this activity aims to continue providing support for NCCs.

Objectives:

- support the operation of the NCCs and to enable them to **support the cybersecurity community**, including SMEs, for the uptake and dissemination of **state-of-the-art cybersecurity solutions and strengthen cybersecurity capacities.** This could also be achieved by using Financial Support for Third Parties (**FSTPs**).
- providing support for the **uptake of EU cybersecurity technologies and products**, commercialisation and **scale-up** of the European cybersecurity start-up/SME ecosystem, in collaboration and complementarity with the European and ongoing **national and regional initiatives**, such as accelerator and incubation programmes and technology transfer programmes.

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC

Scope: ***The NCCs should carry out one or more of the following tasks***

- ✓ *Act as contact points at the national level for the Cybersecurity Competence Community to* **support the ECCC** *in achieving its objectives and missions.*
- ✓ *Provide* **expertise** *and actively contributing to the* **strategic tasks of the ECCC**
- ✓ *Promote, encourage and facilitate the* **participation of civil society and industry in cross-border projects** *and cybersecurity actions funded through all relevant Union programmes.*
- ✓ *Provide* **technical assistance to stakeholders** *by supporting them in their application phase for projects managed by the ECCC.*
- ✓ *Seek to establish* **synergies** *with relevant activities at national, regional and local levels.*
- ✓ *Implement specific actions for which grants have been awarded by the ECCC, including through the provision of* **FSTP**; *Support the* **scaling-up of start-ups** *by finding other funding to implement existing projects.*
- ✓ **Promote** *and* **disseminate** *the relevant* **outcomes** *of the work of the Network and the ECCC*
- ✓ *Assess requests for becoming part of the* **Cybersecurity Competence Community** *by entities established in the same Member State as the NCC.*
- ✓ **Advocate** *and promote involvement in the* **activities** *arising from the ECCC, the Network of National Coordination Centres, and the Cybersecurity Competence Community.*
- ✓ **Support the Cybersecurity Competence Community registration** *(on platforms such as ATLAS) and contribute to the development of suitable community management tools.*

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC

Scope: ***In addition, the NCCs could also carry out one or more of the following tasks***

- ✓ *Provide* **support to innovative ideas towards market-readiness***.*
- ✓ *Promote* **cybersecurity awareness***,* **best practices***, and careers in schools, universities, and community events.*
- ✓ **Strengthen collaboration** *between institutions for higher education, support activities in primary and secondary levels of education to increase cybersecurity awareness and hygiene.*
- ✓ **Build stronger partnerships with established SMEs, tech companies, and government agencies** *to develop and distribute software tools and services that assist in early threat detection, actor identification, and threat evolution monitoring.*
- ✓ **Organise** *periodic cybersecurity* **boot camps, challenges, awareness campaigns and training courses** *across Europe, specifically for SMEs or students. Organise periodic awareness raising campaigns, at national and regional level, and cyber exercises to enhance the security and resilience of critical sectors as well as SMEs.*
- ✓ *Foster a* **community** *of* **cybersecurity professionals** *who can share their experiences, challenges, and solutions.*
- ✓ *Support and encourage the uptake of cybersecurity educational policy goals in national (cybersecurity) strategies.*
- ✓ *Promote safer digital behaviours and more youth considering* **cybersecurity careers.**

The action could also aim to support the adoption of **market-ready innovative cybersecurity solutions***, including those developed in the framework of EU-supported research and innovation projects; and provide and deploy up to date tools and services to organisations (in particular SMEs) to prepare, protect and respond to cybersecurity threats.*

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-NCC

- Indicative duration of the action: 36-48 months
- Type of Action: Simple Grants
- Grant amount: EUR 2-3 million
- Indicative number of projects to be funded: 3
- Type of Beneficiaries: National Coordination Centres and other private and public entities in consortium with NCCs, including academia and research entities.

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CyberHEALTH

Dedicated action to reinforcing hospitals and healthcare providers

Objective:

- strengthen the cybersecurity of **hospitals and healthcare providers**; ensure that hospitals and healthcare providers can effectively **detect, monitor, and respond to cyber threats**, particularly ransomware, thereby enhancing the **resilience** of the European healthcare system.

Scope:

The action will support **pilot projects** *bringing together regional and/or national clusters associations of hospitals/healthcare providers and cybersecurity service providers. The pilot projects will:*

- *define the* **state of preparedness** *of clusters of hospitals and healthcare providers in the EU, to be able to* **assess their needs***; prepare an* **overview of the state-of-the-art cybersecurity solutions and resources** *needed for hospitals and healthcare providers to meet the scope of the action.*
- *develop* **technical plans***, tailored to the needs of representative hospitals and healthcare providers :*
- *conduct a* **demo implementation** *of these technical plans to demonstrate their effectiveness in operations at the stakeholders' sites.*
- *serve as* **demonstration projects and provide cybersecurity education and training to the staff***, enhancing awareness and ensuring best practices in safeguarding sensitive healthcare information.*
- *undertake wide* **dissemination activities** *of best practices across the EU*

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CyberHEALTH

- Indicative duration of the action: 18-24 months
- Type of Action: Simple Grants
- Grant amount: EUR 3-5 million
- Indicative number of projects to be funded: 6
- Type of Beneficiaries: Private and public entities

Consortia shall include regional and/or national clusters of hospitals and healthcare providers from at least two EU Member States (such as national healthcare systems, hospitals or associations of hospitals, healthcare providers and/or professional associations of healthcare practitioners), comprising small, medium and large entities, as well as cybersecurity service providers.

DEP-09 Call topics list

DIGITAL-ECCC-2025-DEPLOY-CYBER-09-CYBERAI

- Cybersecure tools, technologies and services relying on AI

EUR 15 000 000

DIGITAL-ECCC-2025-DEPLOY-CYBER-09-SMEUPTAKE

- Uptake of innovative cybersecurity solutions for SMEs

EUR 15 000 000

DIGITAL-ECCC-2025-DEPLOY-CYBER-09-CYHUBSNAT

- National Cyber Hubs

EUR 20 000 000

DIGITAL-ECCC-2025-DEPLOY-CYBER-09-CYHUBSCRO

- Cross-Border Cyber Hubs

EUR 20 000 000

DIGITAL-ECCC-2025-DEPLOY-CYBER-08-PrepTEST

- Coordinated preparedness testing and other preparedness actions

EUR 5 000 000

Cybersecure tools, technologies and services relying on AI

Objective

- Addresses AI-based technologies (including GenAI) for national authorities and competent authorities, including National and Cross-Border Cyber Hubs, CSIRTs, public bodies and private entities from the NIS 2 directive, NCCs.
- Strengthen capacity to analyse, detect and prevent cyber threats and incidents, support production of high-quality intelligence.
- Tackle risks in AI technologies including misuse, supply chain security, compliance with the AI Act, IPR and GDPR.
- Ensure AI performance, robustness and trustworthiness.

Cybersecure tools, technologies and services relying on AI

Scope

- Develop/deploy systems and tools for cybersecurity based on AI technologies, covering threat/vulnerability detection, threat mitigation, incident recovery, data analysis and sharing.
- Must include at least one of the following: pattern detection, CTI creation, real-time monitoring, malware analysis, vulnerability identification, crossover risk-reduction (AI-IoT-smart grids), self-healing capacities, automated testing, access pattern analysis, anonymised CTI sharing.
- Enable secure AI tools aligned with CRA, contribute to certification.
- Tools made available for licensing to Cyber Hubs, CSIRTs, competent authorities under favourable conditions.

Type of beneficiaries

- Technology providers, Operators of Cyber Hubs, Research and academia, Cybersecurity entities, Public sector, NIS 2 Directive entities, Private sector, Other relevant stakeholders supporting the deployment of cyber-secure AI solutions

Uptake of innovative cybersecurity solutions for SMEs

Objective

- Facilitate market uptake of cybersecurity solutions, especially those from EU-funded R&I.
- Help SMEs adopt tested and validated tools, services, frameworks.
- Support compliance with regulatory requirements, including CRA and NIS 2.

Scope

- Focus on adaptation and deployment of existing market-ready solutions.
- Avoid internal tool development by SMEs; rely on externally developed, validated solutions.
- May involve cooperation with solution providers, intermediaries, authorities.

Type of beneficiaries

- SMEs, Start-ups, Research and academia, Public sector, NIS 2 Directive e
- Industry actors and stakeholders (including solution providers)

National Cyber Hubs

Objective

- Support deployment of National Cyber Hubs under the European Cybersecurity Alert System, as defined in the Cyber Solidarity Act.
- Reinforce national detection, situational awareness and incident response capacities.

Scope

- Activities may include acquisition and deployment of tools, infrastructures and services to strengthen cybersecurity operations.
- Improve maturity, resilience, and secure information sharing.
- Integrate national capacities into EU-wide threat detection and coordination.

Type of beneficiaries

- Competent public authorities designated as National Cyber Hubs, CSIRT
- Other public authorities involved in cyber incident handling or alerting

Cross-Border Cyber Hubs

Objective

- Support deployment of Cross-Border Cyber Hubs under the European Cybersecurity Alert System.
- Facilitate joint situational awareness and response across the EU.

Scope

- Enable procurement and deployment of shared cross-border infrastructures and services.
- Promote coordinated cyber monitoring, joint data exchange, and technical cooperation.
- Improve interoperability and preparedness at EU level.

Type of beneficiaries

- Groupings of at least two public entities from different Member States designated as Cyber Hubs
- CSIRTs, NIS SPOCs and other national authorities tasked with cyber response
- Entities operating shared cybersecurity infrastructures across borders

Coordinated preparedness testing and other preparedness actions

This action covers two actions from the Cyber Solidarity Act, dedicated to the Cybersecurity Emergency Mechanism, namely (1) coordinated preparedness testing of entities operating in sectors of high criticality across the Union and (2) other preparedness actions for entities operating in sectors of high criticality and other critical sectors.

Objectives:

Proposals should contribute to achieving at least one of the following objectives:

- (part 1) Coordinated preparedness testing of entities operating in sectors of high criticality across the Union (including penetration testing and threat assessment) considering ICT as well as Operational Technology/Industrial Control Systems.
- (part 2) Other preparedness actions for entities operating in sectors of high criticality and other critical sectors (i.e. vulnerability monitoring, exercises and training courses).

Coordinated preparedness testing and other preparedness actions

Scope: **Part 1 Coordinated preparedness testing**

✓ ***Support for testing for potential vulnerabilities***

- development of penetration testing scenarios;
- support for conducting testing of essential entities operating critical infrastructure for potential vulnerabilities;
- support for the deployment of digital tools and infrastructures supporting the execution of testing scenarios and for conducting exercises;
- facilitate the execution of cyber-exercises, in particular within cross-border scenarios;
- evaluation and/or testing of cybersecurity capabilities of MS entities and MS sectors, and of entities in scope;
- consulting services, providing recommendations on how to improve infrastructure security and capabilities.

✓ ***Support for threat assessment and risk assessment***:

- Threat Assessment process implementation and life cycle
- Customised risk scenarios analysis.

Coordinated preparedness testing and other preparedness actions

Scope: Part 2 other preparedness actions

✓ ***Support for threat assessment and risk assessment***

✓ ***Risk monitoring service***

✓ ***Support coordinated vulnerability disclosure and management***:

- Promote the adoption of national CVD (Coordinated vulnerability Disclosure) of Policies and the EU Vulnerability Database.
- Coordinate the disclosure of vulnerabilities and timely dissemination of security patches.
- Standardisation of the way information is shared between different stakeholders in the vulnerability handling process.
- CVD applications that manage multiple sources of vulnerability information using open standards or technologies. (e.g. researchers, vendors, CSIRTs)
- Raise awareness on the adoption of vulnerability management best practices.

✓ ***Dedicated exercises and training courses***

Coordinated preparedness testing and other preparedness actions

Type of Beneficiaries:

- For coordinated preparedness testing: Public bodies acting as cybersecurity competent authorities or CSIRTs. Public bodies subject to the NIS 2 Directive, CRA, CSA, CSoA, DORA etc.
- For other preparedness actions: Public bodies acting as cybersecurity competent authorities or CSIRTs, National Cyber Hubs, as identified by the Member States. Public bodies and other entities subject to the NIS 2 Directive (highly critical and other critical sectors entities), CRA, CSA, CSoA, DORA etc. Industry stakeholders, other public and private entities that can support the implementation of the NIS 2 Directive (along with or for highly critical and other critical sectors or entities), CRA, CSA, CSoA, DORA, GDPR, etc. Trusted cybersecurity service providers.

Awards criteria

Relevance

- Alignment with the objectives and activities
- Contribution to long-term policy and strategic objectives
- Extent to which the project would reinforce and secure the digital technology supply chain in the EU*

Implementation

- Maturity of the proposed action
- Soundness and efficiency of the implementation plan
- Capacity of the applicants or consortium to carry out the proposed work

Impact

- Achievement of the expected outcomes and deliverables, as well as communication and dissemination
- Competitiveness strengthen and contribution to society

*__May not applicable to all topics__

Budget categories and costs eligibility

Cost Type	Description	Notes
Personnel Costs	Salaries and wages for staff working on the action, based on actual time and pay.	Includes SME owners/natural persons, seconded persons with unit rate calculation.
Subcontracting Costs	External tasks or services provided by third parties, requiring prior approval.	Must not cover core tasks of the applicant; must be justified.
Purchase Costs (Goods, Works, Services)	Costs for equipment, services, licenses, and other purchases needed for the project.	Must follow best value for money and be necessary for the project.
Travel and Subsistence Costs	Costs for travel and accommodation of staff directly involved in project activities.	Must be justified and directly linked to project activities.
Depreciation Costs of Equipment	Eligible portion of depreciation for equipment used in the action.	Charged only for the portion used for the action.
Other Direct Costs	Direct costs not falling under other categories, such as dissemination or audits.	Must be directly linked and necessary for the action.
Indirect Costs	25% flat rate on eligible direct costs (excluding subcontracting) to cover overheads.	No supporting documentation required.

Other cost categories Financial Support to Third Parties

References

Digital Europe Programme website : https://digital-strategy.ec.europa.eu/en/activities/digital-programme

Digital Europe Programme Regulation: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0694&qid=1621344635377

Funding & tender opportunities portal: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/digital

Call document: under preparation – available at the call opening

Call indicative timelines 2025-2026

Call process	DEP 8	DEP 9
Call opening	June 2025	September 2025
Deadline for submission	October 2025	January 2026
Evaluation	November - December 2025	March - May 2026
Information on evaluation results	February 2026	June 2026
GA signature (target)	July 2026	December 2026

Keep in touch

ⓕ ECCC Newsletter

in ECCC LinkedIn

ECCC Twitter/X

▶ ECCC Instagram

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Thank you!

Europe digitally secured

Area 2 – Implementing the Cyber Solidarity Act

- **Deliver on the Cyber Solidarity Act** by contributing to the consolidation of the European Cybersecurity Alert System.
- **Support the deployment of Cyber Hubs and Cross-Border Cyber Hubs** in line with the recently adopted Cyber Solidarity Act.
- **Support detection and enhance awareness** regarding cybersecurity threats.
- **Implement the Cybersecurity Emergency Mechanism.**
- **Support preparedness actions across Member States,**
- **Support mutual assistance between Member States** in the context of the Cyber Solidarity Act.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE