



TRAFICOM

Liikenne- ja viestintävirasto



Digitaalinen Eurooppa

CYBER-09 rahoitusmahdollisuudet kyberturvallisuuden kehittämiseen

25.11.2025



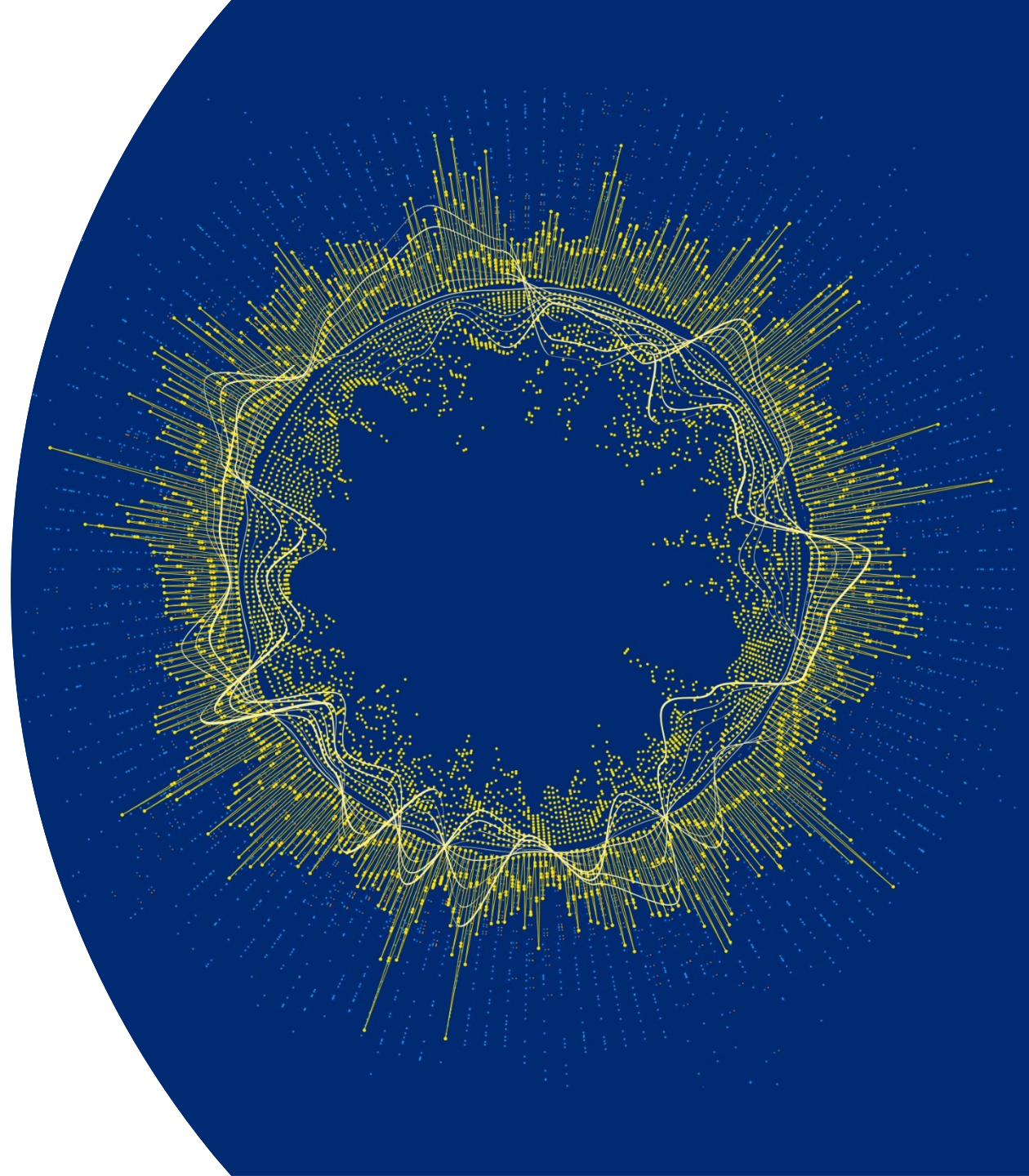
Co-funded by
the European Union



Ohjelma

- ▶ Kansallisen koordinoitikeskuksen palvelut
- ▶ Digitaalinen Eurooppa –CYBER-09 avautuneet rahoitushaut
 - ▶ Cybersecure tools, technologies and services relying on AI
 - ▶ Uptake of innovative cybersecurity solutions for SMEs
 - ▶ Coordinated preparedness testing
 - ▶ Regional Cable Hubs
- ▶ Kysymykset ja vastaukset
- ▶ Tilaisuuden päättäminen

**Kyberturvallisuuden
tutkimuksen,
kehityksen ja
innovaatioiden
kansallisen
koordinoitikeskuksen
(NCC-FI) palvelut**





Kansallisen koordinoitikeskuksen tavoitteena on

- ▶ Edistää unionin kilpailukykyä, johtajuutta ja strategista itsenäisyyttä kyberturvallisuusosalalla
 - ▶ Tukea kansallisesti kyberturvallisuuden tutkimusta, kehitystä ja innovointia
 - ▶ Kasvattaa kansallista kyberturvallisuuskapasiteettia ja valmiuksia suojautua kyberuhilta
 - ▶ Vastata kyberturvallisuusalan osaajapulaan

Euroopan parlamentin ja neuvoston asetus (EU) 2021/887 Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskusten ja kansallisten koordinoitikeskusten verkoston perustamisesta

Miten tuemme suomalaisia toimijoita kyberturvallisuusalan EU-rahoituksen hakemisessa?

- ▶ Kokoamme yhteen keskeiset toimijat Suomessa osaamisyhteisöksi
- ▶ Tiedotamme avautuvista rahoitushauista
- ▶ Tuemme partnereiden etsimisessä ja verkostoitumisessa
- ▶ Ohjeistamme kyberturvallisuusalan rahoitusmahdollisuuksien löytämisessä
- ▶ Tuemme hallinnollisissa prosesseissa ja sopimusasioissa
- ▶ Koulutamme ja tuemme rahoitushakemusten valmistelussa
- ▶ Myönnämme kaskadirahoitusta



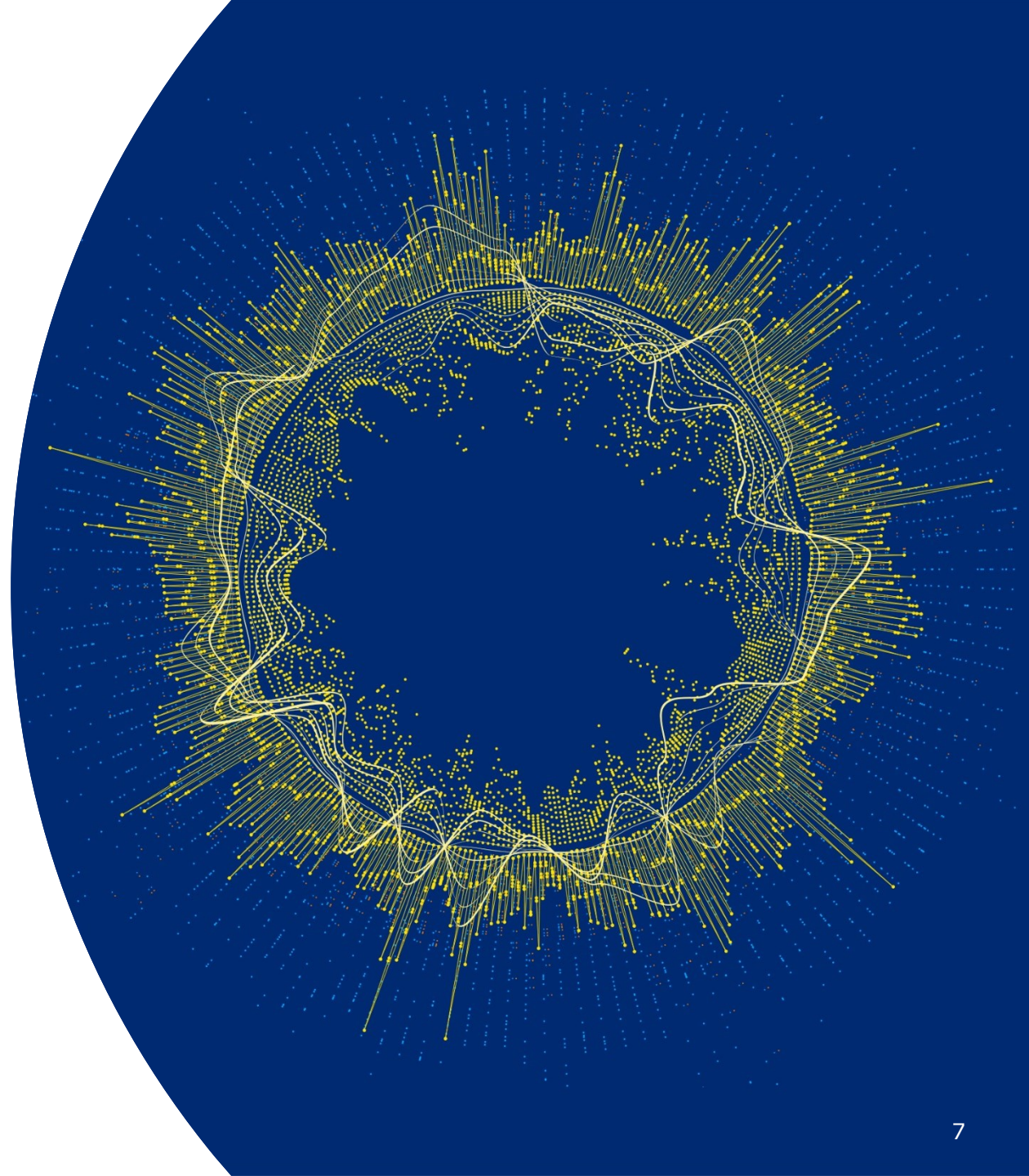
Liity osaamisyhteisöön ja edistä organisaatiosi kansainvälistymistä ja TKI-mahdollisuuksia kyberalalla!



- ▶ Saat ajankohtaista tietoa kyberturvallisuusalan TKI-kehityksestä sekä rahoitusmahdollisuuksista, tukea EU-rahoituksen hakemiseen, kanavia EU-vaikuttamiseen, sekä verkostoitumismahdollisuuksia niin Suomessa kuin Euroopassa.
- ▶ Osana maksutonta osaamisyhteisöä saat kuukausittaisen uutiskirjeen, hankeyhteistyöilmoituksia EU-rahoitushakuihin liittyen sekä kutsuja monipuolisiin tapahtumiin.
- ▶ **Liity mukaan QR-koodin tai [nettisivujemme kautta](#) ja hyödynnä vaikutusmahdollisuudet – kasvata samalla organisaatiosi osaamista!**
- ▶ Lisätietoja: ncc-fi@traficom.fi.

Digitaalinen Eurooppa –kybertyöohjelman avautuneet haut

CYBER-09



Digitaalinen Eurooppa lyhyesti

Mitä rahoituksella tuetaan?

Teknologioiden, tuotteiden ja tutkimustulosten käyttöönottoa ja markkinoille vientiä.

Paljonko rahoitusta jaetaan?

Kyberturvallisuuteen 355 M€ jaettuna vuosille 2025-2027

Kenelle?

Mahdollisuuksia kaikille julkisesta sektorista yksityiseen.

Eryteisesti pk-yrityksiä kannustetaan mukaan.

Mahdollisuus hakea yksin, kansallisena- tai kv-konsortiona.

Projektien kokoluokka?

n. 1-3 vuotta ja n. 3-5 M €/projekti

(Kattaa n. 50-75% kustannuksista)

Tarkemmat tiedot?

[DEP-työohjelmat](#) julkaistu vuosille 2025-2027. Kyberturvallisuudella erillinen työohjelma, jota hallinnoi ECCC.



DEP CYBER-09 rahoituskierrös:

Haut avautuneet 28.10.2025

- ▶ Hakutekstit löytyvät Komission Funding and Tenders portaalista
 - ▶ <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home>

Haettavissa olevat aiheet

- ▶ [Cybersecure tools, technologies and services relying on AI](#)
- ▶ [Uptake of innovative cybersecurity solutions for SMEs](#)
- ▶ [Coordinated preparedness testing](#)
- ▶ [Regional Cable Hubs](#)

Haut sulkeutuvat 31.3.2026!

- ▶ Arvioinnin tulokset kesä- heinäkuussa 2026



Cybersecure tools, technologies and services relying on AI

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

OBJECTIVE: AI-based technologies (including GenAI) for national authorities and competent authorities, including National and Cross-Border Cyber Hubs, CSIRTs, public bodies, private entities from the NIS 2 directive, and NCCs.

These enabling technologies should allow for more effective creation and analysis of Cyber Threat Intelligence (CTI), automation of large-scale processes, as well as faster and scalable processing of CTI and identification of patterns that allow for rapid detection and decision making.

The security of AI itself, especially for the systems in the learning phase, also needs to be addressed, including the misuse of AI by malicious actors. In addition to being secure, the AI technologies being developed should perform well, and be robust and trustworthy.

SCOPE: Actions in this topic should develop and deploy systems and tools for cybersecurity, based on AI technologies, addressing aspects such as threat detection, vulnerability detection, threat mitigation, incident recovery through self-healing, data analysis and data sharing. These activities must also comply with intellectual property rights (IPR) and the GDPR.

EXPECTED OUTCOMES: [E.g. At least one of the following made available to Cyber Hubs, CSIRTs, NCSCs, NIS SPOCs and others. Full list in call text.]

- ▶ Deployment of Artificial Intelligence and various AI-powered technologies
- ▶ Novel cybersecurity tools based on AI that have been developed, tested and validated
- ▶ Enhanced information sharing and collaboration [...] supported by CTI produced by AI-powered tools.
- ▶ Tools for automation of cybersecurity processes e.g. creation, analysis and processing of CTI
- ▶ Original European CTI feeds or services
- ▶ Advanced and innovative secure AI solutions developed and implemented for NIS sectors.
- ▶ Contribution to the standardisation and certification of cybersecure, trustworthy AI technologies.

Tämän esityksen listat lyhennelmiä. Varmista täysi listaus annetuista ehdotuksista hakutekstistä!

Rahoitettavat tahot:

Teknologioiden tarjoajat, Cyber Hubit, akatemia, tutkimuslaitokset, kyberturvallisuustoimijat, NIS2 direktiivin alaiset toimijat, loppukäyttäjät

Rahoitus: Simple Grant 50%

Budjetti: 3-5 M€

Projektin ehdotettu kesto: 3 vuotta

Konsortio: Ei rajoitteita. Konsortiohakemusta suositellaan.

Uptake of innovative cybersecurity solutions for SMEs

DIGITAL-ECCC-2025-DEPLOY-CYBER-09-UPTAKE

The action aims at improving industrial and market readiness for the cybersecurity requirements for SMEs ensuring more secure hardware and software products.

OBJECTIVE: Proposals should contribute to achieving at least one :

- ▶ Availability of innovative tools and services that support SMEs in complying with the EU legislation or reporting incidents and in assisting with recovery if possible.
- ▶ Improved security and notification processes and means in the EU, Improved security of network and information systems in the EU, Industrial and market readiness for CRA, Support for Cybersecurity certification (CSA).
- ▶ Support for supply chain partners in standardised self-assessments and certifications. Helping downstream supply chain partners in a step-by-step approach to increase cyber resilience.
- ▶ Overcome the challenge of finding the technical skills
- ▶ [Cyber toolkit as a service](#) to support for SMEs managing cyber risks, defining, and implementing their cybersecurity strategy, including several functions dedicated to risk assessment, vulnerabilities and threats detection, etc.

SCOPE: The action will focus on supporting at least one of the **EXPECTED OUTCOMES:**

- ▶ The development of a cyber toolkit as a service to support SMEs managing cyber risks, defining, and implementing their cybersecurity strategy
- ▶ Support and incident response capabilities to SMEs
- ▶ Support tools and platforms

Tämän esityksen listat lyhennelmiä. Varmista täysi listaus annetuista ehdotuksista hakutekstistä!

Rahoitettavat tahot: PK-yritykset, julkiset ja yksityiset toimijat jotka toimeenpaneavat NIS2 ja CRA käytänteitä, tutkimus, akatemia, jne.

Rahoitus: SME Support Actions 50%; PK-yrityksille 75%

Budjetti: 3 M€

Projektin ehdotettu kesto: 3 vuotta

Konsortio: Ei rajoitteita. Konsortiohakemusta suositellaan.

Coordinated preparedness testing

DIGITAL-ECCC-2025-DEPLOY-CYBER-09-COORDPREP

This topic covers actions from the Cyber Solidarity Act, dedicated to the Cybersecurity Emergency Mechanism, namely coordinated preparedness testing of entities operating in sectors of high criticality across the Union, specifically the health sector, and in particular hospitals, and the digital infrastructure sector, including electronic communication sector, and in particular fixed networks and submarine cable infrastructure.

OBJECTIVE: [...] to increase the level of protection and resilience to cyber threats, in particular for critical industrial installations and infrastructures, by assisting Member States in their efforts to improve their preparedness for cyber threats and incidents by providing them with knowledge and expertise.

Proposals should contribute to achieving 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.

SCOPE: The provision of preparedness support services shall include the activities listed below, for entities in the sector or sub-sector as identified by the Commission [...].

- ▶ **Support for testing for potential vulnerabilities:** Development of penetration testing scenarios; Support for conducting testing of essential entities; Support for the deployment of digital tools and infrastructures supporting the execution of testing scenarios; Evaluation and/or testing of cybersecurity capabilities of MS entities; Consulting services, providing recommendations on how to improve infrastructure security and capabilities, etc.
- ▶ **Support for threat assessment and risk assessment,** such as Threat Assessment process implementation and life cycle; Customised risk scenarios analysis.

EXPECTED OUTCOMES:

- ▶ Enhanced cooperation, preparedness and cybersecurity resilience in the EU; preparedness support services
- ▶ Threat assessment and risk assessment services.

Tämän esityksen listat lyhennelmiä. Varmista täysi listaus annetuista ehdotuksista hakutekstistä!

Rahoitettavat tahot: CSIRT toimijat ja julkiset reguloidut toimijat (NIS2, CRA, CSA, CSoA, DORA, etc.), muut toimijat konsortiossa

Rahoitettavat toimialat (2025): Terveystieteiden tutkimus - erityisesti sairaalat; digitaalinen infrastruktuuri - erityisesti kiinteät verkot ja merikaapelit

Rahoitus: Simple Grant 50%

Budjetti: 1,5 M€

Projektin ehdotettu kesto: 2 vuotta

Konsortio: Ei rajoitteita. Konsortiohakemusta suositellaan.

Coordinated preparedness testing – haun tarkennus

The Cyber Solidarity Act provides as well that the coordinated preparedness testing should be conducted using common risk scenarios and methodologies that should be developed by the NIS Cooperation Group in cooperation with the Commission, EEAS, ENISA and, within the remit of its mandate, EU-CyCLONE.

[...]

The proposed risk scenarios for this call are in 3 different critical sectors:

- For health sector – risk scenarios affecting hospitals;
- For digital infrastructure sector – risk scenarios affecting submarine cable infrastructures;
- For digital infrastructure sector – risk scenarios affecting fixed networks

[...]

Each applicant may choose among the proposed risk scenarios what they would use for the national action (included in the proposal). However, the proposal should include at least one baseline scenario (which is the first one for each three sub-sectors in annex 3).

Varmista skenaarioiden kuvaukset hakutekstin liitteen 3 kappaleesta 4. Liite sisältää myös ehdotuksen käytettävästä metodologiasta.

Coordinated preparedness testing has 3 main phases:

A. Systemic risk analysis phase

In this phase a more high-level systemic risk assessment:

- ▶ Identify key stakeholders
- ▶ Decide on scope
- ▶ Refine risk scenarios

A. Testing phase

In this phase the testing takes place. This can take the form of:

- ▶ Vulnerability Scanning
- ▶ Security Audits
- ▶ Penetration Testing
- ▶ Exercises
- ▶ (Cyber Resilience) Stress Tests

A. Gap analysis phase

In this phase the coordinated preparedness test results are converted to actionable recommendations:

- ▶ Identify gaps
- ▶ Recommendations
- ▶ Action plan

Regional Cable Hubs

DIGITAL-ECCC-2025-DEPLOY-CYBER-09-CABLEHUBS

As part of the EU Action Plan on Cable Security, it was announced that the Commission, together with voluntary Member States, will work on Cable Integrated Surveillance Mechanisms per sea basin ('Regional Cable Hubs') to enhance the detection capacity against threats to undersea cables as they are critical infrastructure. Taking into account the fact that these cables are covered by the scope of NIS2 Directive that follows an all-hazards approach, it is crucial to protect their physical environment from events such as malicious acts, including cuts as integral part of the cable cybersecurity measures.

OBJECTIVE/SCOPE: The objective is to support the progressive establishment of Regional Cable hubs, one per sea basins of the EU, whose role will be to concretely enhance threats detection and operational security around these strategic infrastructures.

[...] aimed at supporting the set-up of processes, tools and services for detection and analysis of emerging threats, to establish a near real time situational awareness to protect the undersea cables. It includes the capacity to aggregate data and security information from all available sources and analyse them in an automated way.

EXPECTED OUTCOMES:

The Regional cable hubs will contribute to enhancing and consolidating collective situational awareness and capabilities in detection, supporting the development of an operational capacities to ensure the security and resilience of undersea cables. The hubs should:

- ▶ act as a central point allowing for broader pooling of data and information
- ▶ allow a rapid exchange of information, even if classified among participating authorities
- ▶ make use of existing systems which were not developed necessarily for Cable Security
- ▶ integrate direct cooperation with private entities, especially cable operators to increase access to information on ongoing and future threats
- ▶ integrate the defence dimension

Tämän esityksen listat lyhennelmiä. Varmista täysi listaus annetuista ehdotuksista hakutekstistä!

Rahoitettavat tahot:

Julkishallinnot/virastot/tahot jotka ovat vastuussa valtioiden merikaapeli-infrastruktuurista, merialueen turvallisuustoimijat, kyberturvatoimijat, jne.

Rahoitus: Simple Grant 70%

Budjetti: 3 M€

Projektin ehdotettu kesto:
3 vuotta

Konsortio: Vähintään kaksi toimijaa kahdesta eri valtiosta samalta merialueelta. Suositellaan mahdollisimman suurta kattavuutta per merialue.

Koordinointikeskuksen Kohdennetut infotilaisuudet

- ▶ **Uptake of innovative cybersecurity solutions for SMEs**
 - ▶ Keskiviikko 3.12. klo 8.30-9.00
- ▶ **Cybersecure tools, technologies and services relying on AI**
 - ▶ Torstai 4.12. klo 8.30-9.00
- ▶ **Coordinated preparedness testing and other preparedness actions**
 - ▶ Perjantai 5.12. klo 8.30-9.00

Tule mukaan katsomaan hakuteksti yhdessä läpi, esittämään kysymyksiä ja löytämään linjoilta yhteistyökumppaneita.

Ilmoittautumiset jokaiseen erikseen [Koordinointikeskuksen tapahtumat | Kyberturvallisuuskeskus](#) sivustolta.



Vilkaisu vuosiin 2026 ja 2027 DEP kyber –hakujen osalta

- ▶ Vuonna 2026 on odotettavissa haku kyberpuolustustoimijoille "Dual-use Technologies"
- ▶ Vuonna 2026 ja 2027 myös enemmän julkishallinnolle suunnattuja hakuja
- ▶ Työohjelmassa jo esiteltyjä hakuja mm:
 - ▶ Cybersecure tools, technologies and services relying on AI (2026,2027)
 - ▶ Uptake of innovative cybersecurity solutions for SMEs (2027)
 - ▶ Coordinated preparedness testing and other preparedness actions (2026, 2027)
 - ▶ Strengthening cybersecurity capacities of European SMEs with cybersecure AI solutions (2026)
 - ▶ Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements (2026,2027)
- ▶ Muutokset mahdollisia!



Vilkaisu vuosiin 2026 ja 2027 DEP kyber skills –hakujen osalta

- ▶ Parhaillaan auki kaksi hakua (DL: 3.3.2026), jotka toistuvat myös 2026 ja 2027:
 - ▶ ELEVATE: European League of Advanced Digital Skills Academies
 - ▶ European Advanced Digital Skills Competitions
- ▶ Kyberosaamista rahoitetaan lisäksi mm. seuraavista aiheista:
 - ▶ Sectoral digital skills academies
 - ▶ 2026: AI factories
 - ▶ 2027: Semiconductors
 - ▶ Excellence in higher education and training programmes in key digital areas and applied technologies
 - ▶ 2026: Digital Health & Destination Earth)
 - ▶ 2027: Academic excellence in selected key digital areas
 - ▶ Digital Skills and Jobs Platform (jatkohaku)
 - ▶ EdTech Accelerator
- ▶ Muutokset mahdollisia!

Hetki kysymyksille ja vastauksille



Kiitos!

[NCC-FI\(at\)traficom.fi](mailto:NCC-FI(at)traficom.fi)

koordinointikeskus.fi

TRAFICOM

Liikenne- ja viestintävirasto



Co-funded by
the European Union