

**BUSINESS
FINLAND**

TRAFICOM

Liikenne- ja viestintävirasto



Rahoitusmahdollisuudet kyberturvallisuuden kehittämiseen

18.6.2025



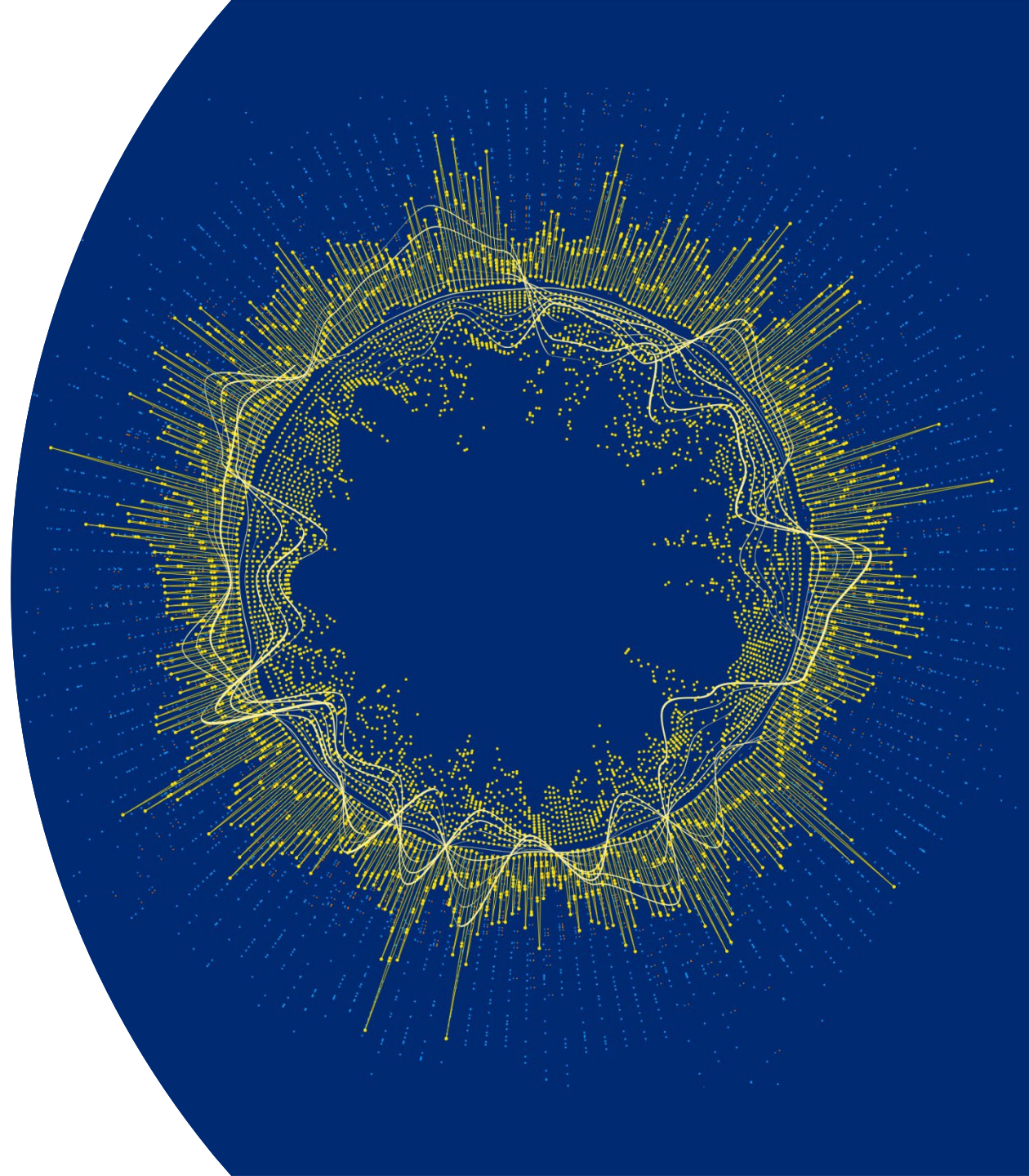
Co-funded by
the European Union

A large, abstract graphic on the left side of the slide, featuring a dense network of glowing blue and white lines and dots, resembling a fiber optic or data network, set against a dark background.

Ohjelma

- ▶ Kansallisen koordinoitikeskuksen palvelut
- ▶ Kansallisesti haettavat rahoitusmahdollisuudet
- ▶ Business Finlandin palvelut kyberalan yrityksille
- ▶ Horisontti Eurooppa -ohjelman rahoitusnäkymät
- ▶ Digitaalinen Eurooppa -kybertyöohjelman rahoitusnäkymät
- ▶ 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 tutkimusosaamiskeskuksen ja kansallisten koordinoitikeskusten verkoston perustamisesta

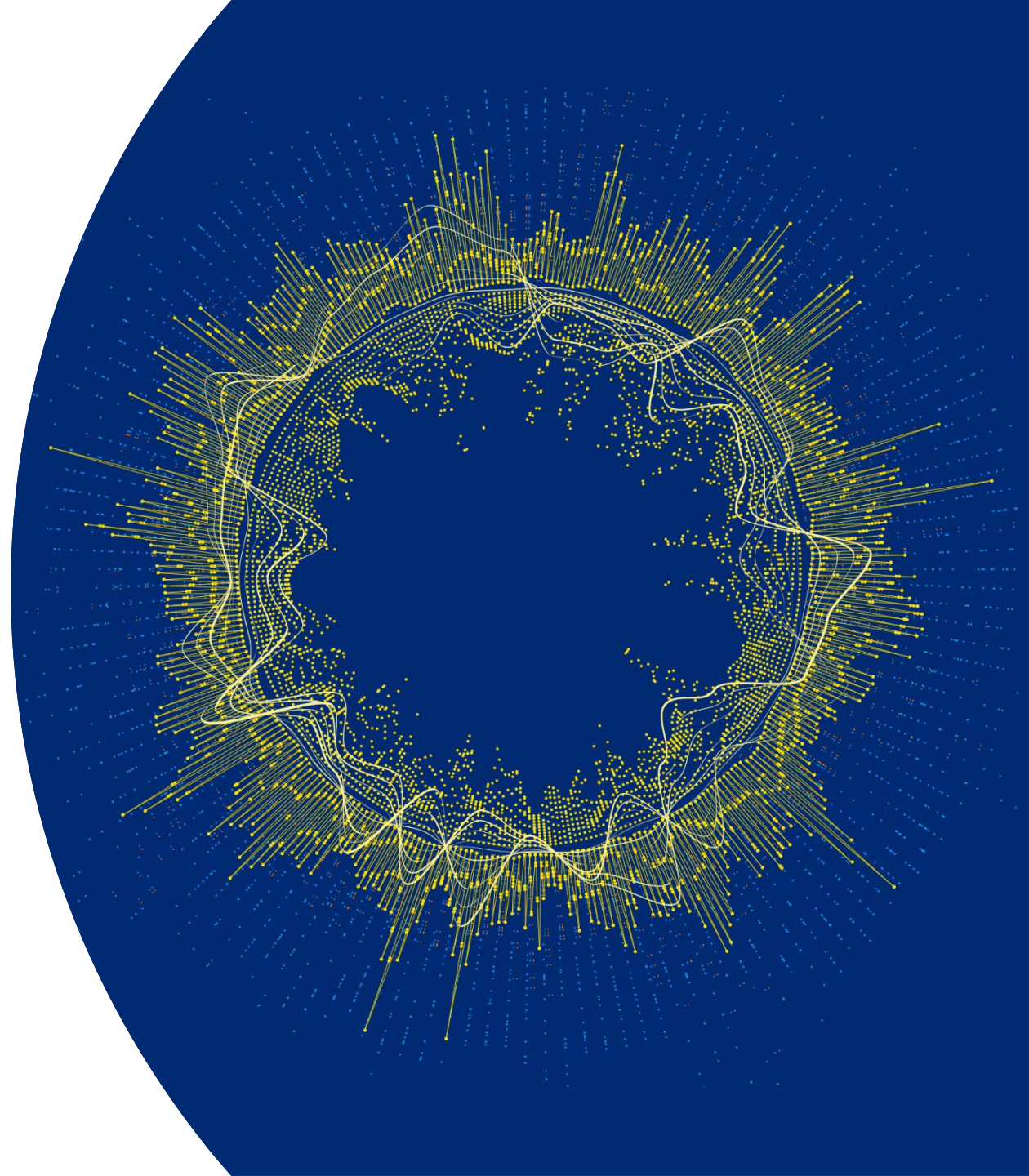
Miten tuemme suomalaisia toimijoita kyberturvallisuusalan EU-rahoituksen hakemisessa?

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

Kuullaksesi lisää liity osaamisyhteisöömme verkkosivuillamme www.koordinointikeskus.fi



Kansallisesti haettavat rahoitusmahdollisuudet ja kaskadirahoitukset





Kansalliset kyberturvallisuuden kehityksen rahoitushaut

- ▶ **Koordinointikeskus myöntää rahoitustukea (FSTP)** vuosina 2025–2029 mm. uusien kybersäädösten toimeenpanon tukemiseksi ja kehittyneiden kyberturvallisuusratkaisujen käyttöönottoon ja levittämiseen.
 - ▶ Ensimmäinen haku kyberturvallisuuslain toimeenpanon tukemiseksi. Haku ja info tulossa Q3/2025.
- ▶ **Haeavustuksia.fi** poimintoja TKI-hauista
 - ▶ [Deep tech accelerator -rahoitushaku: 1.4.–17.8.2025](#) (BF)
 - ▶ [Tutkimusorganisaatioiden ja pk-yritysten yhteistyö: 5.5.–12.12.2025](#) (BF)
 - ▶ [Research to Business – rahoitusta tutkimuslähtöisen idean kaupallistamisen valmisteluun, haku 2/2025: 2.6.–17.9.2025](#) (BF)

Kaskadirahoitukset ts. Financial Support to Third Parties (FSTP)

Tiedotus hauista: EU Funding and Tenders Portal

► CRESCENDO –EU-projekti

- DEP-ohjelmasta rahoitettu pohjoismainen projekti energiasektorin kyberturvallisuushankkeiden rahoittamiseksi
- Projektissa mukana Norja, Tanska sekä Suomi (Traficom)
- Myönnettävän rahoituksen määrä yht. 4 MEUR
- 50 % omavastuurahoitus
- Haut tarkoitettu ensisijaisesti pk-yrityksille
- Ensimmäinen hakukierros syksyllä 2025
- Lisätietoa uutiskirjeissämme

► SECURE –EU-projekti

- DEP-ohjelmasta rahoitettu Unionin laajuinen projekti kyberresilienssisäädöksen (CRA) toimeenpanon tukemiseksi
- Myönnettävän rahoituksen määrä yht. 16,5 MEUR
- Haut tarkoitettu pk-yrityksille
- Ensimmäinen hakukierros syksyllä 2025
- Lisätietoa www.secure4sme.eu

BUSINESS
FINLAND

BUSINESS FINLANDIN PALVELUT KYBERALAN YRITYKSILLE + HORISONTTI EUROOPPA KLUSTERI 4

Kansalliset ja EU-rahoitusmahdollisuudet kyberturvallisuuden kehittämiseen
18.6.2025, webinaari

Otto Vainio

National Contact Point, Horizon Europe Cluster 4 (Digital), Digital Europe Programme

otto.vainio@businessfinland.fi

+358 50 564 8954

DEFENSE AND DIGITAL RESILIENCE - TAVOITTEET

Kansainväliset edelläkävijäratkaisut yhteiskuntien puolustamiseen ja turvallisuuteen tulevat Suomesta

1. Erinomaisia, kilpailukykyisiä ratkaisuja on syntynyt TKI-toiminnan kautta
2. TKI- sekä liiketoimintayhteistyö kansainvälisissä verkostoissa erityisesti EU- ja NATO-maiden kanssa on lisääntynyt selvästi
3. Liiketoiminta ja vienti on kasvanut merkittävästi vetovoimaisten tuotteiden ja palveluiden sekä liiketoimintaekosysteemien ansiosta



Business Finlandin
ohjelma 2024 – 2028

Rahoitustavoite 120 M€

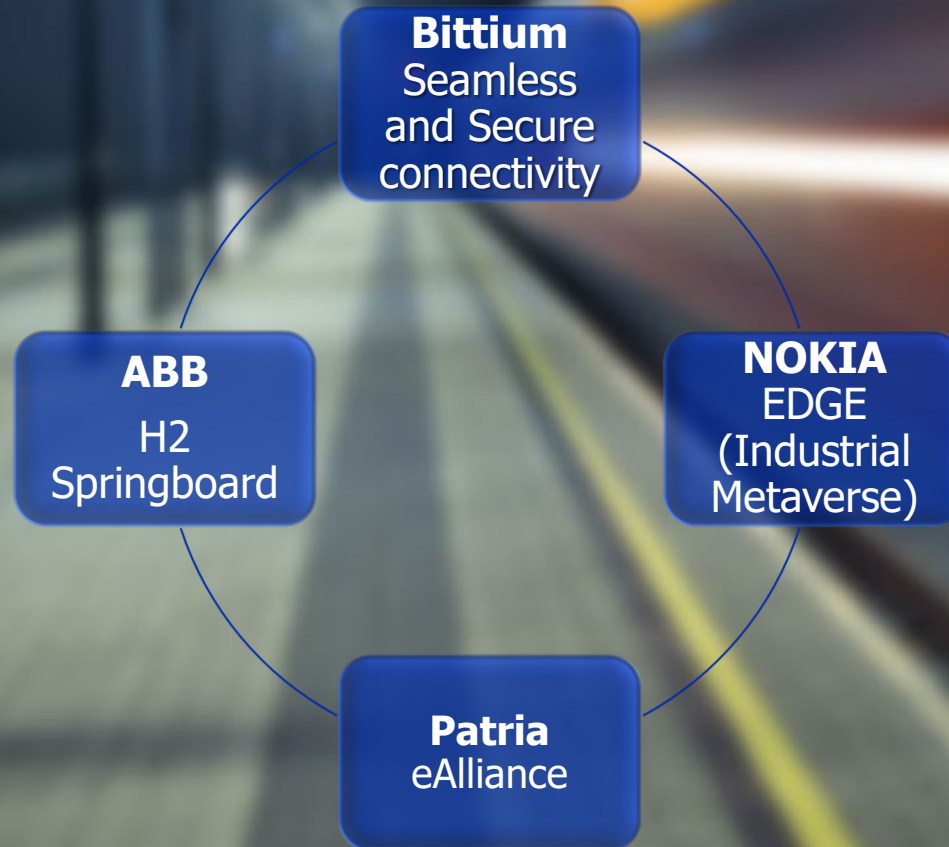


KRIITTINEN VIESTINTÄ (Critical Communication)

SYNERGIAT PUOLUSTUS-, VIRANOMAIS- JA SIVIILISEKTORIN RATKAISUJEN KESKEN

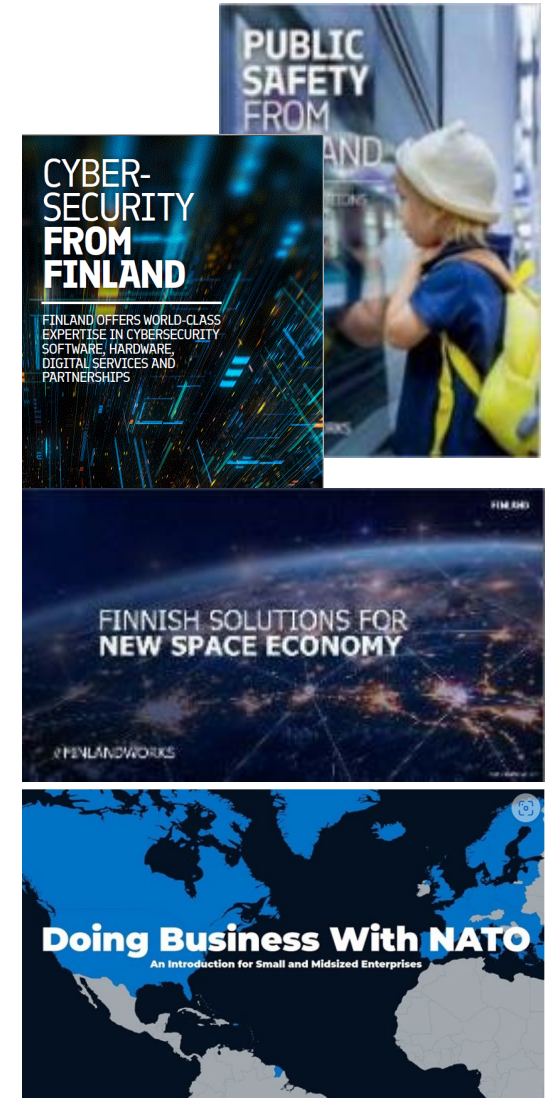
VETURIYRITYKSET 2020-2025

Ainakin seuraavilla veturiyrityksillä on kyberturvallisuuteen liittyvää T&K:ta tiekartallaan



D&DR OHJELMAN KV-KASVUA TUKEVAT PALVELUT

- BF:n Defence and Digital Resilience ohjelman proaktiivisten aktiviteettien kohteina mm. Ruotsi, Norja, UK, Saksa, USA, Australia
- Tiedon jako kv-mahdollisuuksista – markkinatutkimukset, webinaarit
- Kotimaiset verkottumistapahtumat TKI-hankkeisiin ja vientiin liittyen
- Kansainväliset vientidelegaatiot ja tapahtumat sekä viennin toimia tukevat neuvonta- ja rahoituspalvelut (mm. exhibition explorer, market explorer)
- Markkinointi (mm. tarjoomat) ja PR kotimaassa ja kansainvälisesti
- Kansallinen yhteistyö mm. Traficomin ja FISCin kanssa. Esim. Connect4Cyber 27.8. <https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/kansallinen-koordinointikeskus/connect4cyber-brokerage-and-info-day-helsinki-2782025>
- Ohjelman uutiskirje <https://www.businessfinland.fi/defensedigitalresilience>



Horizon Europe CL4 Digital

Cybersecurity opportunities in WP2025

Call ID	Call title	Indicative call budget	EU funding per project	Type of action	Expected TRLs	Opening date	Call deadline
Destination 3							
Connected Collaborative Computing Networks (3C Networks)							
HORIZON-CL4-2025-03-DATA-08	Large-scale pilots for supply end-to-end infrastructures integrating device, network computing and communication capabilities for Telco Edge Cloud deployments, as a basis for Connected Collaborative Computing Networks (3C networks)	75 000 000,00 €	#####	RIA	TRL 3 -> TRL 7	10.6.2025	2.10.2025
AI-GenAI / Data / Robotics							
HORIZON-CL4-2025-03-DATA-13	Fostering Innovative and Compliant Data Ecosystems (AI, Data and Robotics Partnership)	45 000 000,00 €	7 000 000 - 9 000 000 €	IA	TRL 6-7 -> TRL 8	10.6.2025	2.10.2025
Destination 4							
Quantum and High Performance Computing							
HORIZON-CL4-2025-03-DIGITAL-EMERGING-03	Supporting Digital Partnerships in Quantum technologies ("Korea collaboration")	8 000 000,00 €	2 500 000 - 2 700 000 €	RIA	TRL 2-3 -> TRL 3-4	10.6.2025	2.10.2025
AI-GenAI / Data / Robotics							
HORIZON-CL4-2025-03-DIGITAL-EMERGING-07	Robust and trustworthy GenerativeAI for Robotics and industrial automation	85 000 000,00 €	40 000 000 - 45 000 000 €	RIA	TRL 2 -> TRL 6	10.6.2025	2.10.2025
HORIZON-CL4-2025-04-DIGITAL-EMERGING-04	Assessment methodologies for General Purpose AI capabilities and risks (AI/Data/Robotics Partnership)	7 000 000,00 €	3 000 000 - 4 000 000 €	RIA	TRL 2 -> TRL 5	10.6.2025	2.10.2025

OHJELMAN UUTISKIRJE

<https://www.businessfinland.fi/suomalaisille-asiakkaille/palvelut/ohjelmat/defense-digital-resilience>

Kirsi Kokko

Head of Defense and Digital Resilience

Email: kirsi.kokko@businessfinland.fi

Phone: +358 50 550 2023

Horizon Europe Cyber Call2025

18 June 2025

Pauli Stigell, Business Finland

050 5577 856

HORISONTTI EUROOPPA

— EU:N TUTKIMUS- JA INNOVAATIO-OHJELMA —

Pillar 1

Excellent Science

European Research Council

Marie Skłodowska-Curie
Actions

Research Infrastructures

Pillar 2

Global Challenges and
European Industrial
Competitiveness

Clusters

- Health
- Culture, Creativity and Inclusive Society
- Civil Security for Society
- Digital, Industry and Space
- Climate, Energy and Mobility
- Food, Bioeconomy, Natural Resources, Agriculture and Environment

Joint Research Centre

Pillar 3

Innovative Europe

European Innovation Council

European innovation
ecosystems

European Institute of
Innovation
and Technology

Widening Participation and Strengthening the European Research Area

Widening participation and spreading excellence

Reforming and Enhancing the European R&I system



Pillar 2

Global Challenges and
European Industrial
Competitiveness

8,2 mrd. €

2,3 mrd. €

1,6 mrd. €

15,3 mrd. €

15,1 mrd. €

9 mrd. €

2 mrd. €

- Health
- Culture, Creativity and Inclusive Society
- Civil Security for Society
- Digital, Industry and Space
- Climate, Energy and Mobility
- Food, Bioeconomy, Natural Resources, Agriculture and Environment

Joint Research Centre

Cyber 350 M€

Six sections (destinations) of Civil Security research

1. Destination – Better protect the EU and its citizens against **crime and terrorism**
2. Destination – Effective management of EU external **borders**
3. Destination – **Resilient infrastructure**
4. Destination – Increased **Cybersecurity**
5. Destination – A **Disaster**-Resilient Society for Europe
6. Destination – Strengthened Security Research and **Innovation**

DESTINATION 4 – DG CNNECT, ECCC, others by DG HOME

Call 2025

TOTAL 20 topics with 57 projects and 224,15 M€ budget

HORIZON-CL3-2025-FCT-01:	37 M€	3 topics	12 projects
HORIZON-CL3-2025-BM-01	27 M€	3 topics	9 projects
HORIZON-CL3-2025-INFRA-01	22 M€	2 topics	5 projects
"HORIZON-CL3-2025-CS-01"	90,6 M€	6 topics	16 projects
HORIZON-CL3-2025-DRS-01	32 M€	3 topics	8 projects
HORIZON-CL3-2025-SSRI-01	15,6 M€	5 topics	7 projects

Open 12 June 2025

Closes 12 November 2025 (5 kk)

Call – Increased Cybersecurity: HORIZON-CL3-2025-02-CS-ECCC

- HORIZON-CL3-2025-02-CS-ECCC-01: **Generative AI** for Cybersecurity applications, RIA, budget 40 M€, 3 projects
- HORIZON-CL3-2025-02-CS-ECCC-02: New advanced tools and processes for **Operational Cybersecurity**, RIA, budget 23,55 M€, 4-5 projects
- HORIZON-CL3-2025-02-CS-ECCC-03: **Privacy** Enhancing Technologies, RIA, budget 11 M€, 3 projects
- HORIZON-CL3-2025-02-CS-ECCC-04: Security evaluations of **Post-Quantum Cryptography** (PQC) primitives, RIA, 4 M€, 2 projects
- HORIZON-CL3-2025-02-CS-ECCC-05: Security of implementations of Post-Quantum Cryptography **algorithms**, RIA, 6 M€, 2-3 projects
- HORIZON-CL3-2025-02-CS-ECCC-06: Integration of Post-Quantum Cryptography (PQC) **algorithms into high-level protocols**, RIA, budget 6 M€, 2-3 projects

Overall budget: **90,55 mil. €**

Brussels and online on the 11-12 June 2025

Registration for the **ONSITE** participation: [Home | Cluster 3 Infoday and Brokerage Event 2025](#)

Work programme https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/horizon-europe-work-programmes_en#pre-publication-of-work-programme-2025

Earlier brockarage (May, in Paris) by SMI2G

<https://www.cmine.eu/page/smi2g-2025> look at the presentattions

Participant Portal info, BF training

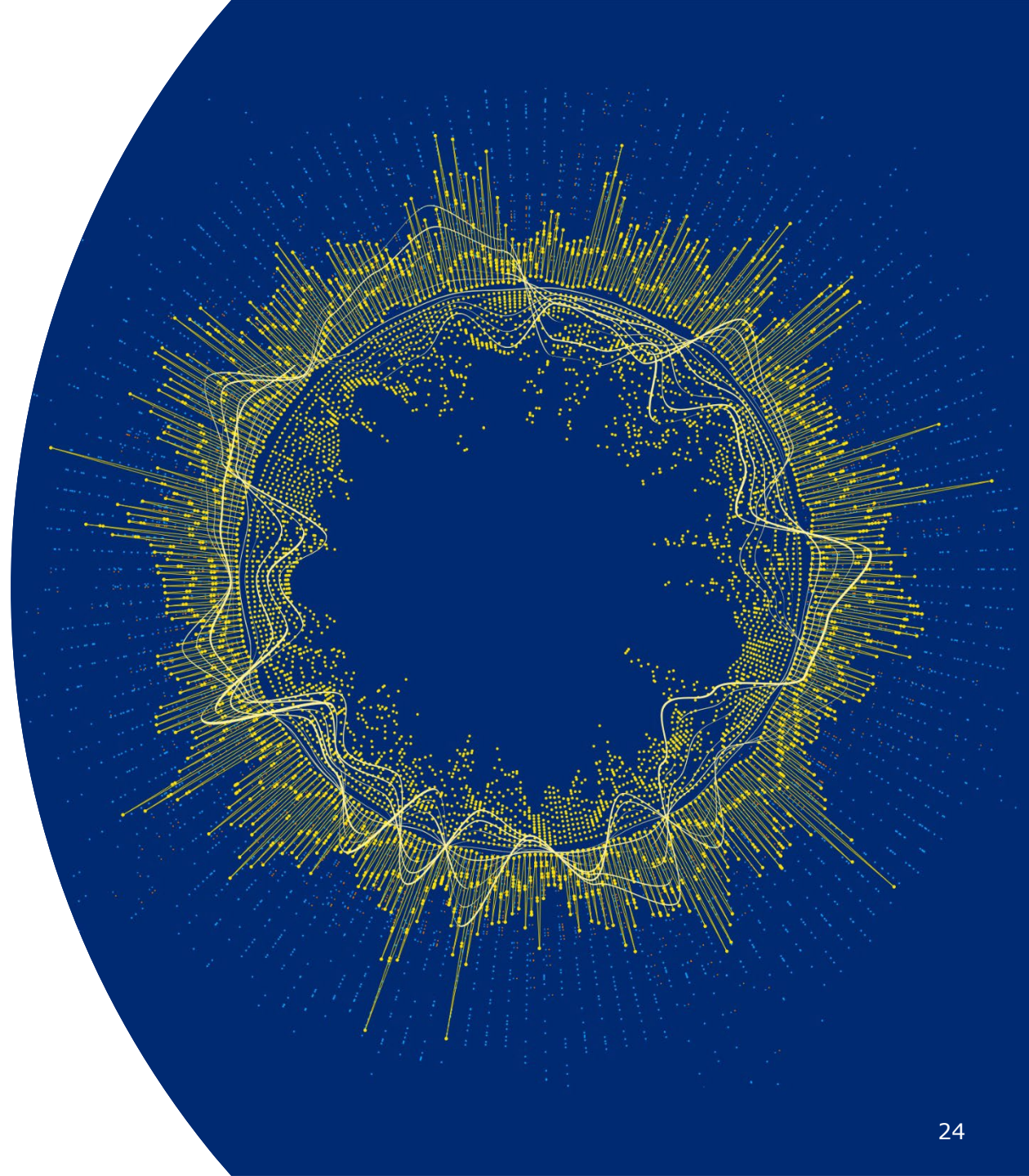
- Latest Call text – the **proposal must answer to its requirements**
 - Other documents that help, give guidance
- Portal lists interested parties but not all are relevant actors!
 - <https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/how-to-participate/topic-announcements/44114300>
- **Old funded projects** <https://cordis.europa.eu/>
- 3 countries minimum (EU and e.g. Norway and UK) - typically 6-12 countries with one or two actors per country.
- **Business Finland training**
 - <https://www.businessfinland.fi/ajankohtaista/tapahtumat/horizontti-eurooppa/2022/save-the-date-horizontti-eurooppa-kustannusasioiden-masterclass>

THANKS

HORISONTTI EUROOPPA

— EU:N TUTKIMUS- JA INNOVAATIO-OHJELMA —

Digitaalinen Eurooppa –kybertyöohjelman rahoitusnäkymät



Digitaalinen Eurooppa lyhyesti

Mitä rahoituksella tuetaan?

Teknologioiden, tuotteiden ja tutkimustulosten käyttöönottoa ja markkinoille vientiä.

Paljonko rahoitusta jaetaan?

Kyberturvallisuuteen 390 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 kyber -rahoitusta avoimna vuonna 2025 seuraavien teemojen alla:

- ▶ Siirtyminen uusiin teknologioihin, generatiivinen tekoäly ja kvanttiturvallisuus
- ▶ Kybersolidaarisuussäädöksen implementointi
- ▶ EU:n kyberturvallisuusresilienssin kehittäminen
- ▶ Erityinen haku terveysalan kyberturvallisuusratkaisuihin

Tämän lisäksi kannattaa tutustua myös päätyöohjelmaan, jossa rahoitusta mm. kyberkoulutukseen ja osaamiseen

Huom. Muutokset työohjelmiin mahdollisia.

Vuonna 2025:

- ▶ 1. hakukierros: 12.6.-7.10.2025
- ▶ 2. hakukierros: Q4/2025 – Q1-2/2026



Kaikille toimijoille soveltuvat DEP-kyberrahoitushaut 2025

Alla olevat haut auki 12.6.-7.10.2025 EU Funding & Tenders portaalissa

Dedicated action to reinforcing hospitals and healthcare providers

- **support pilot projects**, which will bring together stakeholders such as regional and/or national clusters associations of hospitals and healthcare providers as well as cybersecurity service providers.
- International consortium required

Transition to post-quantum Public Key Infrastructures

- **design of digital signature combiners and key encapsulation mechanism combiners**
- **testing of deployment of certificates** in protocols that use those certificates
- the **development of novel protocols** for Automatic Certificate Management and revocation and of novel protocols for certificate-transparency
- the development of methods and tools that can be used by experts across various PKI domains, including **all aspects of key management of asymmetric systems.**

Dedicated action to reinforcing hospitals and healthcare providers

OBJECTIVE: [...] strengthen the cybersecurity of hospitals and healthcare providers. The goal is to ensure that hospitals and healthcare providers, which are crucial operators in the health sector, can effectively detect, monitor, and respond to cyber threats, particularly ransomware, which pose significant risks, thereby enhancing the resilience of the European healthcare system.

SCOPE: This action addresses the growing need for continuous cybersecurity monitoring, threat intelligence, and incident response in hospitals and healthcare providers, which often lack dedicated cybersecurity resources to adequately protect themselves from cyber threats. The action will support pilot projects, which will bring together stakeholders such as regional and/or national clusters associations of hospitals and healthcare providers, as well as cybersecurity service providers. The pilots will develop technical plans, tailored to the needs of representative hospitals and healthcare providers which will also need to include best implementation recommendations and cost estimates for effective deployment. The pilot projects will conduct a demo implementation [...].

EXPECTED OUTCOMES:

- ▶ Mapping of common cybersecurity needs of hospitals and healthcare providers.
- ▶ Guidelines for healthcare providers to assess their current state of cybersecurity protection and relevant needs.
- ▶ Technical cybersecurity plans to enhance preparedness and cyber resilience: improved detection and response capabilities for healthcare institutions minimising the impact of cyberattacks, particularly for ransomware. This also includes dedicated training courses to staff.
- ▶ Pilot cybersecurity demo installations at partner hospitals and healthcare provider sites to ensure hospitals and healthcare providers can maintain operational continuity in the face of cybersecurity incidents. This should be monitored through specific KPIs.
- ▶ Wide dissemination campaigns to help scale up preparedness of hospitals and healthcare providers in Europe.

Rahoitettavat tahot: Ei rajoitteita, mutta konsortion tulee sisältää esim.sairaala tai terveydenhuoltopalvelujen tarjoaja vähintään kahdesta EU-maasta, sekä kyberturvallisuuden palveluntarjoajia

Rahoitus: Simple Grant 50%

Budjetti: 30 M€ (tuki 3-5 M€ per projekti)

Projektin ehdotettu kesto: 1,5-2 vuotta

Avoinna: 12.6-7.10.2025

Linkki: [DIGITAL-ECCC-2025-DEPLOY-CYBER-08-CYBERHEALTH](#)

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.
- ▶ the testing of deployment of certificates in protocols that use those certificates.
- ▶ the development of novel protocols for Automatic Certificate Management and revocation and of novel protocols for (privacy-friendly) certificate-transparency.
- ▶ the development of methods and tools that can be used by experts across various PKI domains, including all aspects of key management of asymmetric systems.

EXPECTED OUTCOMES: [E.g. Full list in call text.]

- ▶ New combiners ensuring that cryptographic schemes provide at least 128-bit security against quantum adversaries.
- ▶ Experimental evaluation on hybrid certificates in several standard protocols that use those certificates, also considering options for different cryptographic algorithms at the root Certification Authority level and at the other levels, in terms of security, performance, and backward compatibility.
- ▶ New and/or improved open-source libraries for certificate requests, issuance, validation, revocation and (privacy-friendly) certificate transparency.
- ▶ Clear procedures taking into account all aspects of key management [...]
- ▶ Test and evaluation of uses of X.509 certificates [and] alternatives to X.509 certificates.
- ▶ Etc.

Rahoitettavat tahot: Kaikki Public Key Infrastructures - arvoketjun toimijat

Rahoitus: Simple Grant 50%

Budjetti: 15 M€ (tuki 3-4 M€ per projekti)

Projektin ehdotettu kesto: 3 vuotta

Avoinna: 12.6-7.10.2025.

Linkki: [DIGITAL-ECCC-2025-DEPLOY-CYBER-08-PUBLICPQC](#)

Kaikille toimijoille soveltuvat DEP-kyberrahoitushaut 2025

Mahdollisesti auki toisen hakukierroksen aikana Q4/2025 – Q1-2/2026

Deployment of a European testing infrastructure for the transition to PQC

- **creating and maintaining a European PQC testing infrastructure.**
- The testing infrastructure should offer a **physical space for in-situ testing**. This **includes the possibility for providing remote testing** for different European stakeholders.
- **Proposals should build on results from ongoing activities in the EU.**

Cybersecure tools, technologies and services relying on AI

- 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.

Uptake of innovative cybersecurity solutions for SMEs

- improving industrial and market readiness for the **cybersecurity requirements set in the Cyber Resilience Act** bolstering cybersecurity rules to **ensure more secure hardware and software products**

Vain tietyille organisaatioille soveltuvat DEP-kyberrahoitushaut 2025

Mahdollisesti auki toisen hakukierroksen aikana Q4/2025 – Q1-2/2026

Coordinated preparedness testing

- **Only for public bodies acting as cybersecurity competent authorities or CSIRTs. Public bodies subject to the NIS2 Directive, CRA, CSA, CSoA, DORA etc.**
- 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.
- Preparedness support services; threat assessment and risk assessment services.
- NB. Part 2 “other preparedness actions” of the call opening in 2026.

Vilkaisu vuosiin 2026 ja 2027 DEP kyber –hakujen osalta

- ▶ Eri vuosien haut eivät ole täysin identtisiä
- ▶ Vuonna 2026 on odotettavissa haku kyberpuolustustoimijoille "Dual use of Technologies"
- ▶ Vuonna 2026 ja 2027 enemmän julkishallinnolle ja kansallisille SOC:eille suunnattuja hakuja
- ▶ Kaikille toimijoille soveltuvia hakuja olisi tulossa seuraavasti:
 - ▶ Cybersecure tools, technologies and services relying on AI (2025,2026,2027)
 - ▶ Strengthening cybersecurity capacities of European SMEs with cybersecure AI solutions (2026)
 - ▶ Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements (2026,2027)
 - ▶ Uptake of innovative cybersecurity solutions for SMEs (2025, 2027)



Kiitos!

NCC-FI(at)traficom.fi

koordointikeskus.fi

**BUSINESS
FINLAND**

TRAFICOM

Liikenne- ja viestintävirasto

Save the date

- [Connect4Cyber – Brokerage
and Info Day, Helsinki
27.8.2025](#)