TLP:CLEAR

ECCC

EUROPEAN CYBERSECURITY COMPETENCE CENTRE

European Cybersecurity Competence Centre (ECCC) and Network and their funding opportunities

Speakers (BSI/CERT-Bund):
Heiko Siebel
Sirko Höer

EU Regulation of ECCC, NCC Network & Cybersecurity Community

TLP:CLEAR

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1 European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) based in Bucharest/Rumania

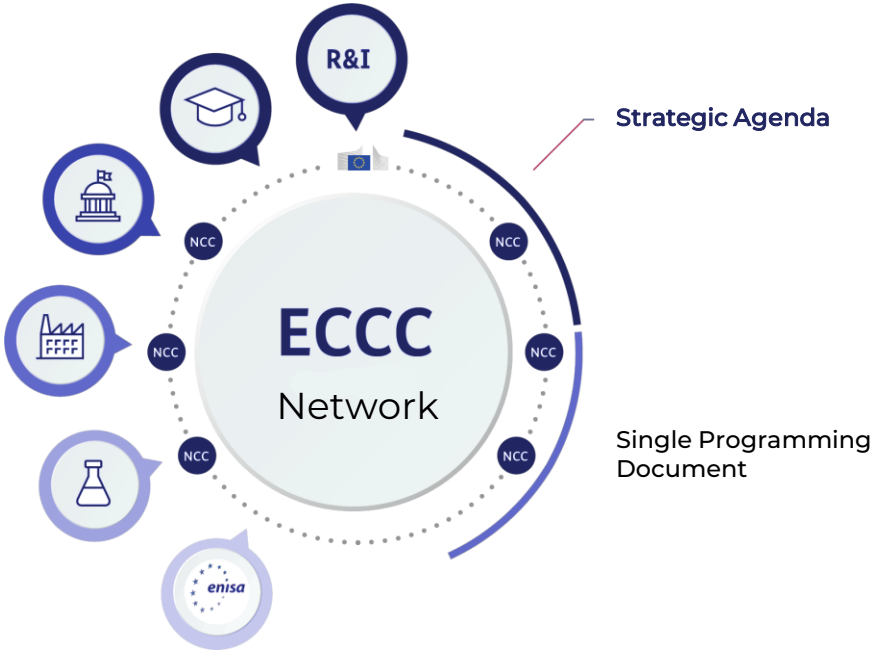
2 National Coordination Centres (NCC) in the EU Member States, nomination until December 29, 2021

National Cybersecurity Community

Industry, Technology & Research

3 Cybersecurity Community addresses concerns of industry, small and medium-sized enterprises (SMEs), start-ups and academia

Structure of the ECCC Ecosystem



ECCC Organisation Entities

- **Governing Board** provides strategic orientation and oversees ECCC activities
- **Executive Director** is the ECCC's legal representative and is responsible for its day-to-day management
- **Strategic Advisory Group** ensures a comprehensive, ongoing and permanent dialogue between the Community and the ECCC

NCC Network

- National Coordination Centres (NCC) are public sector entities in each EU member state
  - Mostly state owned or performing public administration functions
- NCCs support the European Competence Center for Cybersecurity (ECCC)
- Engage national cybersecurity community
  - Industry,
  - academic and research,
  - public sector
- List of confirmed NCCs: https://cybersecurity-centre.europa.eu/nccs_en
  - Currently 24 NCC teams (29th September 2022)

National Coordination Centre Services

Community Building

Contributions to **EU funding programmes** Horizon Europe & Digital Europe

Information about opportunities of EU cybersecurity funding programmes

Support of the cybersecurity community to **apply for EU funding programmes**

EU Funding Programme Horizon Europe (2021-2027)

Excellent Science

- European Research Council
- Marie-Sklodowska-Curie Actions
- Research Infrastructure

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

Innovative Europe

- European Innovation Council
- European Innovation Ecosystems
- European Institute of Innovation and Technology

Cybersecurity topics

Widening participation and strengthening the European Research Area

- Widening participation and spreading excellence
- Reforming and enhancing the EU research and innovation system

EU Funding Programme Digital Europe (2021-2027)

High Performance Computing

- Procure exascale machines
- Upgrade existing supercomputers,
- Quantum computing
- Widen the access to and use of supercomputing

Cybersecurity

- Deploy competence centres network
- Cybersecurity shield, quantum communication infrastructure - QCI
- Certification schemes
- Cybersecurity tools

European digital innovation hubs

- At least one per MS
- At least one per MS on AI

Artificial intelligence, Cloud & Data

- Data4EU : common Data Spaces, cloud, platforms and infrastructure
- Large Testing and Experimentation Facilities in five areas
- Scale up the European AI platform to access tested AI technologies

Advanced Digital Skills

- Master courses
- Short term trainings
- Job placements
- Platform for Skills and Jobs

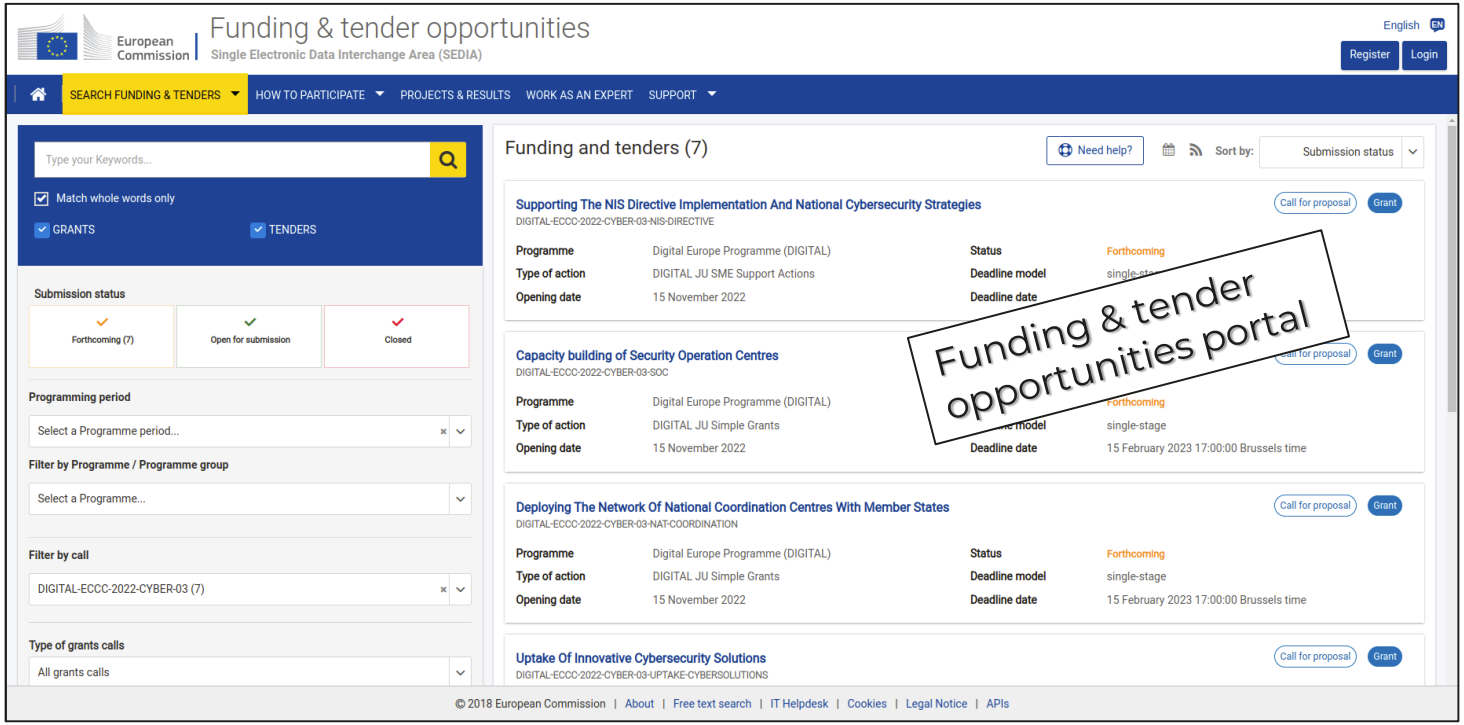
Deployments and Best Practices

- Destination Earth
- Green and smart communities and mobility
- Continuation of investments (CEF – ISA2)
- Once-only principle
- Blockchain
- Enhancing confidence in the digital transformation

Cybersecurity topics in Horizon Europe & Digital Europe 2021-2022

„Horizon Europe“ Cluster 3 / Work Programme 2021-2022	„Digital Europe“ Cybersecurity Work Programme 2021-2022
• Hardware, software and supply chain security	• Secure Quantum Communication Infrastructures (QCI)
• Secure and resilient digital infrastructures and interconnected systems	• Actions for Cybersecurity and Trust - European „Cyber Shield“ - Support To Implementation Of Relevant EU Legislation
• Cybersecurity & disruptive technologies	
• Human-centric security, privacy and ethics	
• Smart and quantifiable security assurance and certification shared across Europe	

Identify suitable Horizon Europe & Digitale Europe funding & tender opportunities



https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-search

Call for tendersHorizon Europe
Cluster 3/Destination 4: Increased Cybersecurity 2021-2022

Topic	Budget (Mio. Euro)	Open	Deadline
Secure and resilient digital infrastructures and interconnected systems			
Improved monitoring of threats, intrusion detection and response in complex and heterogeneous digital systems and infrastructures (IA)	**21,0**	**30.06.2022**	**16.11.2022**
Hardware, software and supply chain security			
Trustworthy methodologies, tools and data security "by design" for dynamic testing of potentially vulnerable, insecure hardware and software components (RIA)	**17,3**	**30.06.2022**	**16.11.2022**
Cybersecurity and disruptive technologies			
Transition towards Quantum-Resistant Cryptography (IA)	**11,0**	**30.06.2022**	**16.11.2022**
Smart and quantifiable security assurance and certification shared across Europe			
Development and validation of processes and tools used for agile certification of ICT products, ICT services and ICT processes	**18,0**	**30.06.2022**	**16.11.2022**

EU Funding & Tender Opportunities Portal:
https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-search;typeCodes=0,1,2,8;statusCodes=31094501,31094502;programCcm2Id=43108390;destination=43650699

Call for tenders Digital Europe: Cybersecurity Work Programme 2021/2022

Topic	Budget (Mio. Euro)		Funding rate	Open	Deadline
Actions for Cybersecurity and Trust: European "Cyber-Shield"					
EU Cybersecurity Resilience, Coordination and Cybersecurity Ranges	15		75 % (SME), others: 50 %	15.11.2022	15.02.2023
Capacity Building Of Security Operation Centres (SOC); (1) Capacity building activity & (2) Deployment and running of advanced tools and infrastructures	(1) 80	(2) 30	(1): 50 % (2): up to 80 %	15.11.2022	15.02.2023
Securing 5G Strategic Digital Infrastructures And Technologies	10		50 %	15.11.2022	15.02.2023
Uptake Of Innovative Cybersecurity Solutions	32		75 % (SME), others: 50 %	15.11.2022	15.02.2023
Actions for Cybersecurity and Trust: Support To Implementation Of Relevant EU Legislation					
Supporting The NIS Directive Implementation And National Cybersecurity Strategies	20		75 % (SME), others: 50 %	15.11.2022	15.02.2023

EU Funding & Tender Opportunities Portal:
https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-search;callCode=DIGITAL-ECCC-2022-CYBER-03

Application Forms for Horizon Europe

Part A (online forms)

1. General Information
2. Participants
3. Budget
4. Ethics and Security
5. Other Questions

Part B (project description, document upload)

Max. 45 pages

1. Excellence
2. Impact
3. Implementation

Application Forms for Digital Europe

Part A (online forms)

1. General Information
2. Participants
3. Budget

Part B (project description, document upload)

Max. 70 pages

1. Relevance
2. Implementation
3. Impact
4. Work Plan, Work Packages, Timing and Subcontracting
5. Others
6. Declarations

Keep in touch

National Coordination Centre for Cybersecurity

c/o Federal Office for Information Security
Section TK 21 – Technology and Research Strategy
Godesberger Allee 185-189
53175 Bonn
Germany

E-Mail: nkcs@bsi.bund.de
Website: https://bsi.bund.de/dok/nkcs