Cybersecurity in the Digital Europe Programme

DG CONNECT

January 2022

#DigitalEuropeProgramme

Challenges in Cybersecurity

- Geopolitical contest over cyberspace
- Large increase in cybercrime
- Supply chain security (e.g. 5G)
- Expanding attack surface (e.g. IoT; hospitals, vaccine distribution)
- Threat from quantum computing breaking “legacy” crypto
- Advent of AI
- Skills shortage; awareness

- Capacity building, resilience
- Vulnerability of smaller organisations, SMEs
- Info sharing, joint analysis and response
- Commercialisation of R&D
- Uptake
- Single market
- Dual use
- (…)

DIGITAL
EUROPE
PROGRAMME

The EU's Cybersecurity Strategy for the Digital Decade (December 2020)

RESILIENCE, TECHNOLOGICAL SOVEREIGNTY AND LEADERSHIP

- Revised Directive on Security of Network and Information Systems (NIS 2)
- Cybersecurity Shield (CSIRT, SOC)
- Secure Communication Infrastructure: Quantum, NG Mobile, IPv6, DNS
- Competence Centre and Network of Coordination Centres (CCCN)
- EU workforce upskilling

BUILDING OPERATIONAL CAPACITY TO PREVENT, DETER AND RESPOND

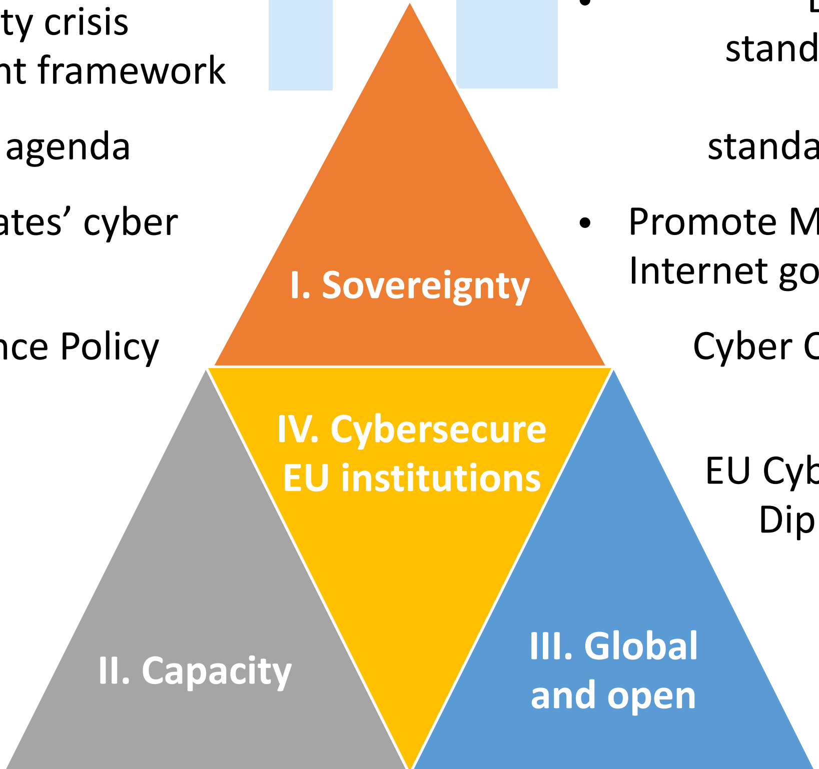
- Cybersecurity crisis management framework
- Cybercrime agenda
- Member States' cyber intelligence
- Cyber Defence Policy Framework

COOPERATION TO ADVANCE A GLOBAL AND OPEN CYBERSPACE

- EU leadership on standards, norms and frameworks in standardisation bodies
- Promote Multi-Stakeholder Internet governance model

Cyber Capacity Building Agenda

EU Cyber Dialogue and Diplomacy Network



Resilience, sovereignty, leadership

Infrastructure	Adopt NIS 2.0
Cyber Shield	Develop Network of Security Operations Centres
Ultra secure connectivity	Quantum enabled encryption
5G networks	Complete implementation of Toolbox
Internet security	Develop DNS4EU
Supply chain autonomy	Encourage EUR 4.5 bn investment across digital supply chain through Competence Centre and Network
Skills	Eg investment in business resilience against cyber-enabled IP theft

Operational capacity: prevent, deter, respond

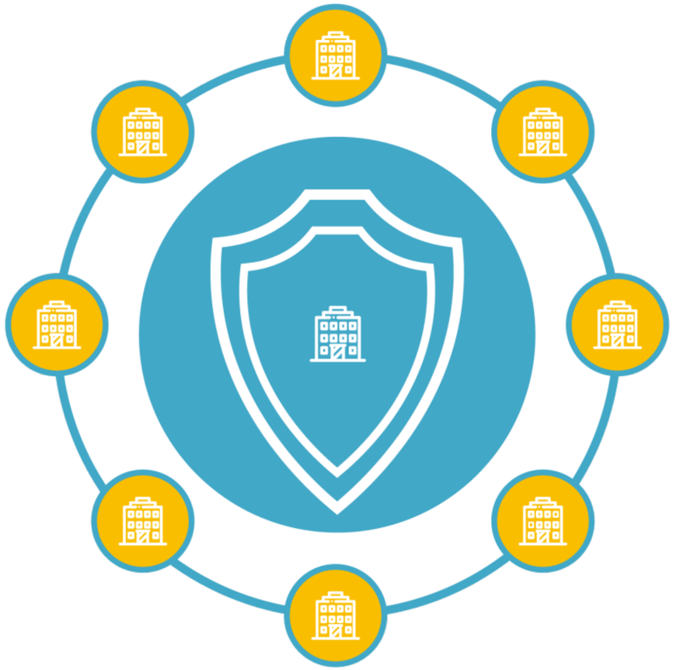
Joint Cyber Unit	Milestones and process to be set out Feb 2021
Cybercrime	Complete Security Union agenda
Cyberdiplomacy toolbox	Strengthen cyber deterrence posture and shared situational awareness Explore additional measures, and increase cooperation with international partners Review Implementing Guidelines
Cyber Defence	Review the Cyber Defence Policy Framework to increase cyber defence cooperation and coordination Encourage Member States’ cyber defence capability development, notably through PESCO and EDF

Global and open cyberspace

EU leadership on international norms and standards	Step-up EU engagement on international standardisation, i.e. ITU Take forward the Programme of Action to Advance Responsible State Behaviour in CyberspacePromote the Budapest Convention and engage in multilateral discussions Promote and protect human rights and fundamental freedoms online
Cooperation with partners	Strengthen and expand cyber dialogues with third countries, regional and international organisations Reinforce regular and structured exchanges with the multi-stakeholder community Form an informal EU Cyber Diplomacy Network with EU “cyber attachés” around the world to promote the EU vision of cyberspace
Strengthen global capacities to tackle cyber threats	Develop an EU External Cyber Capacity Building Agenda Set-up an EU External Cyber Capacity Building Agenda Board Priorities on Western Balkans, EU’s neighborhood and partner countries experiencing a rapid digital development

Specific objectives for ‘Cybersecurity and Trust’

- Build-up advanced cyber equipment, tools, data infrastructures
- Cyber knowledge, capacity and skills; sharing of best practices
- Wide deployment of state of the art cyber solutions across economy
- Capabilities Member States and private sector to comply with NIS Dir.
- Improve resilience against cyber attacks
- Cooperation between civilian and defence regarding dual use



European Competence Centre:

- manage the funds foreseen for cybersecurity under Digital Europe and Horizon Europe 2021-2027
- facilitate and help coordinate the Network and Community to drive the cybersecurity technology agenda
- support joint investment by the EU, Member States and industry and support deployment of products and solutions.

Network of National Coordination Centres:

- Nominated by Member States as the national contact point
- Objective: national capacity building and link with existing initiatives
- National Coordination Centres may receive funding
- National Coordination Centres may pass on financial support

Competence Community:

- A large, open, and diverse group of cybersecurity stakeholders from research and the private and public sectors, including both civilian and defence sectors

- **European Cyber-shield (177M)**
  - EU cybersecurity resilience, coordination and Cybersecurity Ranges
  - Capacity building of Security Operation Centres (SOCs)
  - Securing 5G Strategic Digital Infrastructures and Technologies
  - Uptake of innovative Cybersecurity Solutions
  - Support To Cybersecurity In The Health Sector
- **Support to implementation of relevant EU Legislation (83M)**
  - Deploying the Network of National Coordination Centres with Member States
  - Cybersecurity Community support
  - NIS Directive Implementation and National Cybersecurity Strategies
  - Testing and Certification Capabilities

EU cybersecurity resilience, coordination and Cybersecu Ranges (1/2)

Objective:

- Capacity to monitor cyber-attacks, threats and supply chain risks; react jointly against large-scale incidents,
- Knowledge, skills and training.
- Create, interconnect and strengthen Cybersecurity ranges at European, national and regional level

Link with

- Blueprint; CSIRTs network; Cyber Crisis Liaison Organization Network (CyCLONe); future Joint Cybersecurity Unit

EU cybersecurity resilience, coordination and Cybersecur Ranges (2/2)

Outcomes and deliverables

- Capacity to react in a coordinated way to large scale cybersecurity incidents,
- Top-level cybersecurity ranges offering advanced skills, knowledge and testing platforms.

Main target groups: Public authorities in Member States; enterprises; education and training organisations

Type, indicative budgets, deadline: SME support grant, EUR 15 million, 2-4 million per grant, ca. 36 months duration, deadline January 2023

Capacity building of Security Operation Centres (SOCs) (1/

Objective & Scope

- The objective will be to create, interconnect and strengthen national and regional Security Operation Centres (SOCs) of critical infrastructure or functions at regional, national and EU level.
- Improve cybersecurity resilience with faster detection and response to cybersecurity incidents whether due to a cyber-attack or any other causes, at national and EU level.
- Use of some relevant disruptive technologies such as AI.

DIGITAL EUROPE PROGRAMME

Capacity building of Security Operation Centres (SOCs)(2/

Outcomes and deliverables

Deployment of world-class SOCs across the Union.

Main target groups

National, regional or sectoral SOCs serving private (SMEs in particular) and/or public organisations, public authorities, including competent authorities and CSIRTs under the NIS Directive.

Type, indicative budget, deadline: Simple grant, EUR 80 million, 7-10 million per grant, 36 months, deadline January 2023

Capacity building of Security Operation Centres (SOCs)(3/

Joint procurement

- Call for expression of interest to select entities in Member States that provide the necessary facilities to host and operate cross-border platforms.
- Pooling data on cybersecurity threats between Member States
- Building on this expression of interest, a joint procurement will be launched to develop and operate capacities for the selected cross-border platforms

Type, indicative budget: procurement, EUR 30 million

Securing 5G Strategic Digital Infrastructures and Technologies (1/2)

Objective

- Support relevant entities in Member States’, such as regulators of electronic communications or security agencies, in the implementation of their national cybersecurity strategies and legislation, in line with 5G security policy
- Knowledge and capacity building for relevant national authoritities, e.g. exchange of best practices; staff trainings; deployment of innovative evaluation methods; support standardisation actions; procurement of specialised services (e.g., audit and technical assessments)

Projects involving national authorities from several EU Member States will be prioritised.

Securing 5G Strategic Digital Infrastructures and Technologies (2/2)

Outcomes and deliverables

- Trusted and secure 5G services.
- Support the cooperation between national authorities and private providers of technology services or equipment, in particular innovative European SMEs in cooperation with network and technology providers on piloting, testing and integration of security and interoperability aspects of 5G interoperable, open and disaggregate solutions.

Main target groups

Relevant national authorities may associate themselves with private providers of technology services or equipment, in particular European SMEs, possibly in cooperation with network and technology providers.

Type, indicative budget, deadline: Simple grant, EUR 10 million, 1-3 million per grant, 12-36 months, deadline January 2023

Uptake of Innovative Cybersecurity Solutions (1/2)

Objective and scope

- Market uptake and dissemination of innovative cybersecurity solutions (notably from SMEs, as well as results from public-funded research in the EU),
- Improve knowledge and cybersecurity preparedness.
- Improve awareness
- Testing and auditing
- Coordinated Vulnerability Disclosure
- Hackathons
- …

Uptake of Innovative Cybersecurity Solutions (2/2)

Outcomes and deliverables

- Adoption of market-ready innovative cybersecurity solutions;
- Provide and deploy up to date tools and services to organisations (in particular SMEs);
- Improve the security of open source solutions
- …

Main target groups: Enterprises (in particular SMEs), public authorities, associations
Type, indicative budget, deadline: SME support grant, EUR 32 million, 2-5 million per grant, up to 36 months duration, deadline January 2023

- **European Cyber-shield (177M)**
  - EU cybersecurity resilience, coordination and Cybersecurity Ranges
  - Capacity building of Security Operation Centres (SOCs)
  - Securing 5G Strategic Digital Infrastructures and Technologies
  - Uptake of innovative Cybersecurity Solutions
  - Support To Cybersecurity In The Health Sector

- **Support to implementation of relevant EU Legislation (83M)**
  - Deploying the Network of National Coordination Centres with Member States
  - Cybersecurity Community support
  - NIS Directive Implementation and National Cybersecurity Strategies
  - Testing and Certification Capabilities

Deploying the Network of National Coordination Centres with Member States (1/2)

Objective

- In line with the regulation that created the European Cybersecurity Industrial, Technology and Research Competence Centre
- Implement Cybersecurity Competence Centre and Network Regulation: NCC tasks
- Foster the Cybersecurity Competence Community in each Member State
- Foster cross-border cooperation and the preparation of joint actions

Deploying the Network of National Coordination Centres with Member States (2/2)

Outcomes and deliverables

- Setup and operation of National Coordination Centres in Member States
- Optional: financial support to third parties, for uptake and dissemination of state-of-the-art cybersecurity solutions

Target group: National Coordination Centres with confirmed capacity (as per regulation)

Type, indicative budget, deadline: Simple grant to nominated beneficiaries, EUR 55 million, 2 million per grant, 24 months, deadline May 2022 and January 2023

Cybersecurity Community Support (1/2)

Objective

- Community building in cybersecurity research, technology, and industrial policy at EU level
- Support the European Cybersecurity Competence Centre and the Network of National Coordination Centres
- Build on prior contractual Public Private Partnership on Cybersecurity and on four pilot projects on cybersecurity competence networks

Cybersecurity Community Support (2/2)

Outcomes and deliverables

- Strengthen internal market in Cybersecurity products and services
- Support to Cybersecurity start-ups and scale-ups
- Support to education, training, and gender balance
- Support awareness raising
- …

Type, indicative budget: Procurement, EUR 3 million, 24 months

Supporting the NIS Directive Implementation and Nationa Cybersecurity Strategies (1/2)

Objective

- Development of trust and confidence between Member States;
- Effective operational cooperation of organisations entrusted with EU or Member State’s national level Cybersecurity
- Better security and notification processes
- Improved security of network and information systems in the EU;
- More alignment and harmonisation of Member States’ implementations of the NIS Directive.

Supporting the NIS Directive Implementation and Nationa Cybersecurity Strategies (2/2)

Outcomes and deliverables

Proposals are expected to deliver on at least two of the following results:

- enable the Member States to limit the damage of cybersecurity incidents, while reducing the overall costs of cybersecurity
- improve compliance with the NIS Directive, higher levels of situational awareness and crisis response
- contribute to enhanced cooperation, preparedness and cybersecurity resilience of the EU.

Main target groups

Relevant Member State competent authorities implementing the NIS Directive, CSIRTs (including sectorial CSIRTs), SOCs, OESs, DSPs, industry stakeholders (including ISACs), and any other actors within the scope of the NIS Directive.

Type, indicative budgets, deadline: SME support grant (75% co-funding rate for SMEs and 50% for all the other beneficiaries), EUR 20 million, 1-5 million per grant, 36 months, deadline January 2023

Testing and certification capabilities (1/2)

Objective

- Increase and facilitate security and interoperability testing capabilities and certification of connected ICT systems.
- Improve the capabilities and cooperation of cybersecurity certification stakeholders in line with the objectives of Regulation (EU) 2019/881 (“Cybersecurity Act”).

Possible activities include support for capacity building, for testing and certification of products, standardization actions and testing capabilities for 5G disaggregated and open solutions.

Where relevant, support will focus on certification schemes under the Cybersecurity Act, while it could also be available for technical areas not yet covered by schemes under the Cybersecurity Act.

Testing and certification capabilities (2/2)

Outcomes and deliverables

- The funding is expected to:
- Improve the cybersecurity and interoperability testing capabilities in all Member States;
- Support SMEs to audit their infrastructure in view of improving their cybersecurity protection.
- Actions in the area of standardisation

Main target groups: National cybersecurity certification authorities, conformity assessment bodies and accreditation bodies. National Coordination Centres created on the basis of the Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres may respond to this open call with a view to allocating Financial Support to Third Parties.

Type, indicative budget, deadline: Grant for Support to Third Parties, EUR 5 million, 0.5-1 million per grant, 36 months, deadline January 2023

DIGITAL
EUROPE
PROGRAMME

Call document - Support to proposers

- Details on **admissibility and eligibility**
- Information for applicants on **financial and operational capacity**
- Exclusion criteria
- **Evaluation procedure**
- Guarantees, obligatory milestones and deliverables, certificates and any many other description on legal conditions to participate in grants
- Financial support to third party schemes and conditions
- All the **mandatory annexes** needed for the call (e.g. ethic issues, security issues)
- **Type of action** description
- Other important legal and operational provisions
- **Help for applicants** and how to reach out to the commission

Award criteria: 1. Relevance

- Alignment with the **objectives and activities**
- Contribution to **long-term policy and strategic objectives**
- Reinforcement of the Union’s **digital technology supply chain***
- Resilience to **financial obstacles***

* call document sets applicability

Award criteria: 2. 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

Award criteria: 3. Impact

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

* call document sets applicability

Topics and deadlines upcoming topics

Topic	Budget	Opening	Deadline
Network of National Coordination Centres	€ 55M (total)		
EU cybersecurity resilience, coordination and cybersecurity ranges	€ 15M	29 September	24 January 2023
Capacity building of Security Operation Centres (SOCs)	€ 110M		
Secure 5G and other strategic digital infrastructures and technology	€ 10M		
Uptake of innovative cybersecurity solutions in SMEs	€ 32M		
NIS Directive implementation and national cybersecurity strategies	€ 20M		
Testing and certification capabilities	€ 5M		

Useful links

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