



EU Cybersecurity Strategy and Financial Support

Martin Übelhör
European Commission - DG CONNECT
H1, Cybersecurity Technology and Capacity Building

28 April 2020

Cybersecurity - A strategic priority for the EU



"it is not too late to achieve technological sovereignty in some critical technology areas... Digitalisation and cyber are two sides of the same coin"

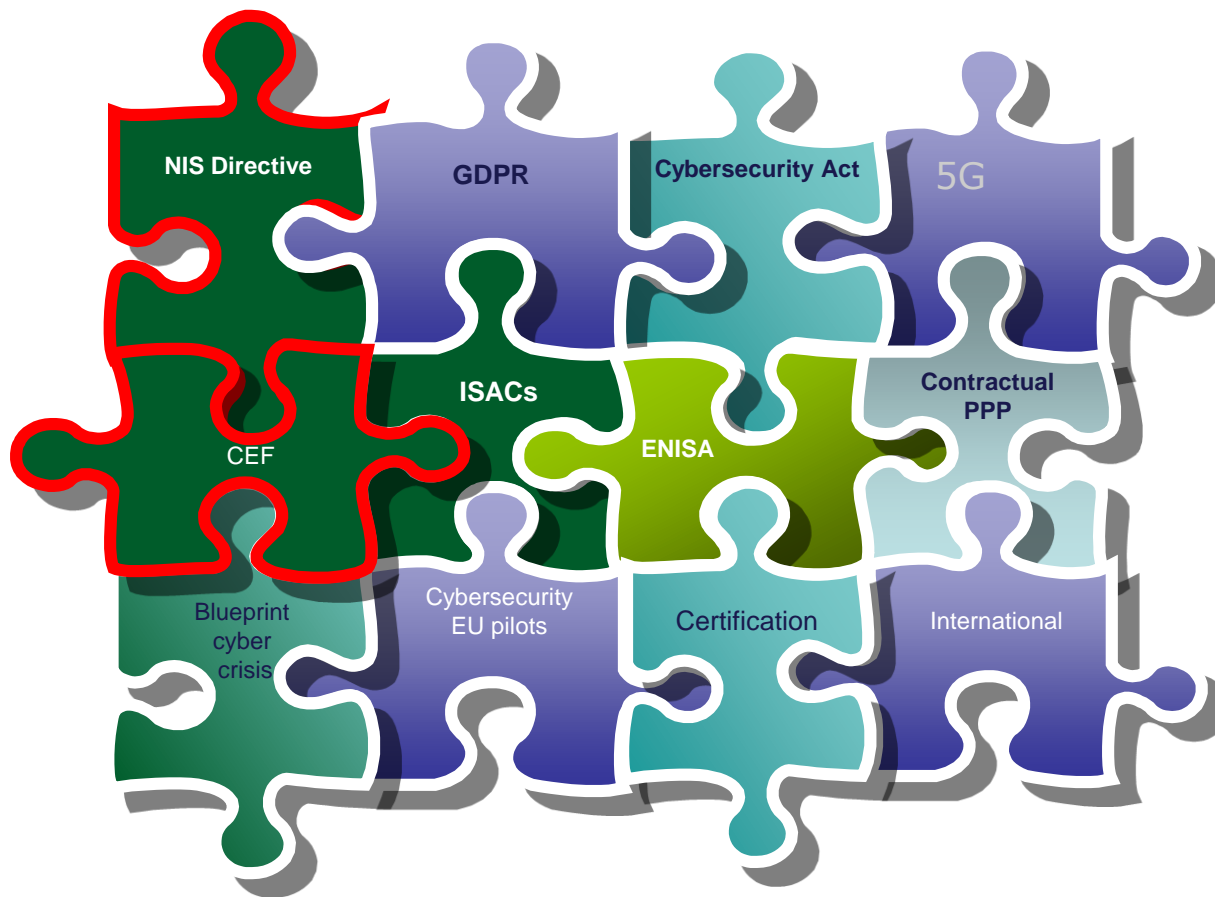
Extract of political guidelines of U von der Layen (priority 3: "A Europe fit for the digital age")



"enhancing Europe's technological sovereignty. ... building a real single market for cybersecurity, notably looking at certification, implementing rules on security of network and information systems, rapid emergency response strategies and other relevant areas. You should lead the work to build a joint Cyber Unit to better protect ourselves."

Extract of mission letter of Commissioner Breton

EU instruments for cybersecurity

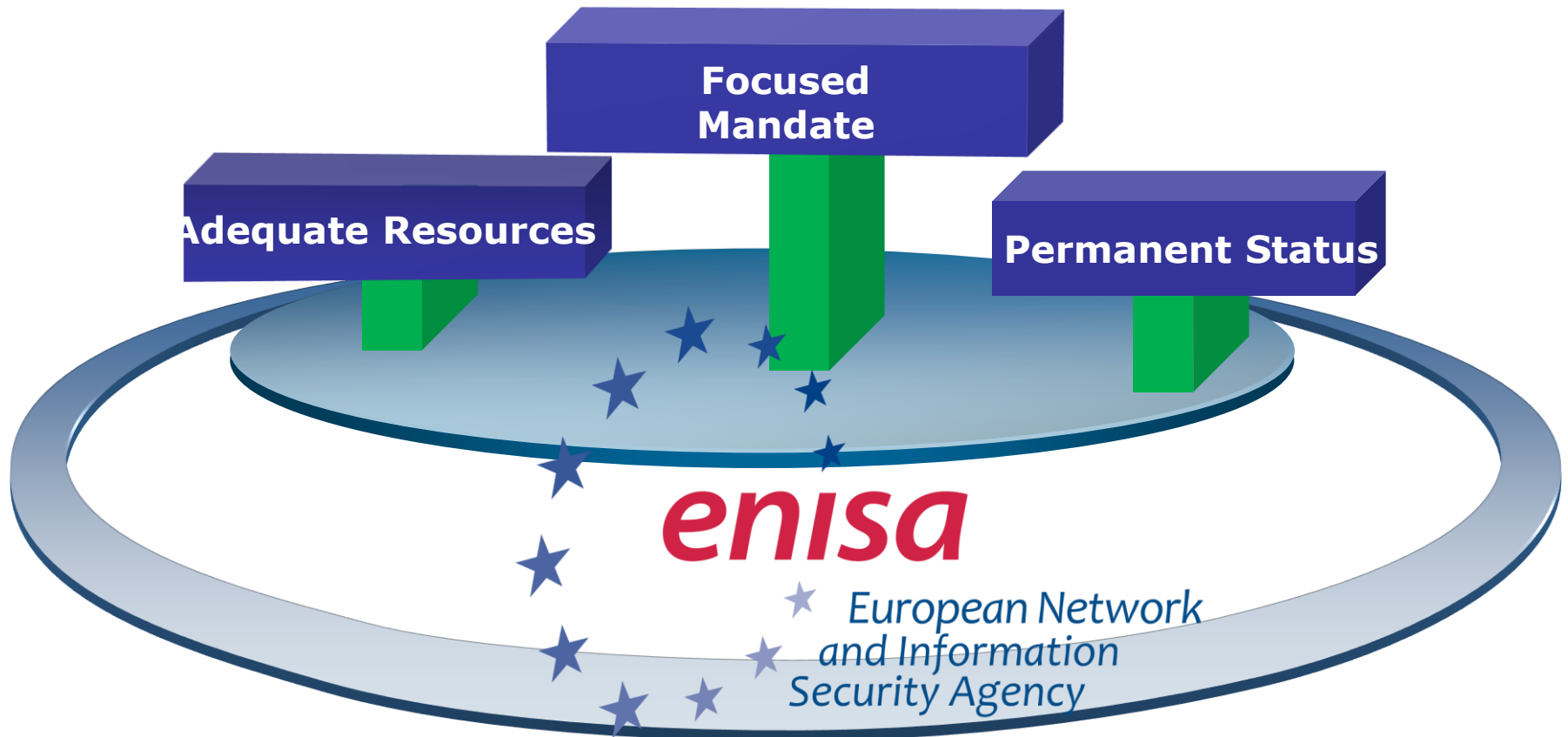


EU Cybersecurity Act

**Towards a reformed
EU Cybersecurity Agency**

**and reinforcing the cybersecurity
single market in the EU**

What's new with the new proposal?



Some highlights of ENISA's work



Organisation of Cyber Europe, the pan-European exercise



ENISA Annual Threat Landscape report: overview of threats, current and emerging trends



Secretariat of the NIS CSIRTs Network



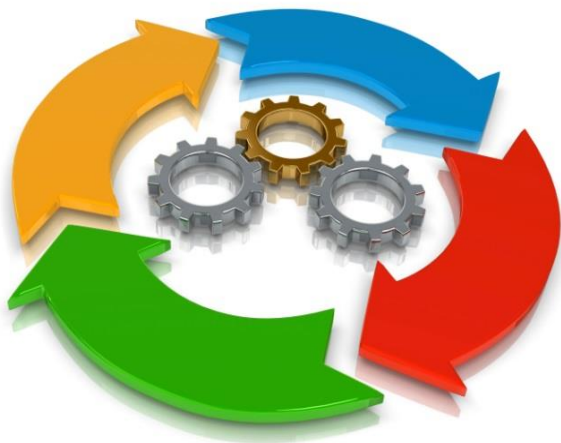
Organisation of the yearly European Cybersecurity Challenge between national teams



Organisation of the yearly European Cybersecurity Month Awareness Campaign

Cybersecurity Certification

A **voluntary European** cybersecurity certification **framework....**



*...to enable the creation of
tailored EU cybersecurity
certification schemes for ICT
products and services...*

...that are valid across the EU





The NIS Directive

The First EU Cybersecurity Law

NIS Directive

The First EU Cybersecurity Law

Boosting the overall cybersecurity in the EU

- Increased national cybersecurity capabilities
- Security & Notification requirements
- National Cybersecurity Strategies
- National Computer Security Incident Response Teams

EU Level Cooperation:

- NIS Cooperation Group
- CSIRTs Network

NIS Directive: Main Features



GREATER CAPABILITIES

Member States have to improve their cybersecurity capabilities.

NATIONAL COMPUTER SECURITY
INCIDENT RESPONSE TEAM (CSIS-
RT)

NATIONAL NIS STRATEGY

NATIONAL NIS AUTHORITY



COOPERATION

Increased EU-level cooperation

EU MEMBER STATES
COOPERATION GROUP
(STRATEGIC)

EMERGENCY TEAMS
(CSIRTS) NETWORK
(OPERATIONAL)



EU MEMBER STATES; EUROPEAN COMMISSION;
EUROPEAN UNION AGENCY FOR NETWORK AND
INFORMATION SECURITY



EU MEMBER STATES; CERT-EU; EUROPEAN
UNION AGENCY FOR NETWORK AND
INFORMATION SECURITY



RISK MANAGEMENT

Operators of essential services and Digital Service Providers have to adopt risk management practices and notify significant incidents to their national authorities.

SECURITY MEASURES

NOTIFICATION OF
MAJOR INCIDENTS

Work Streams 1/2



**Work Stream
1:
Identification
of OES**



**Work Stream
2: Security
Requirements**



**Work Stream
3: Incident
notification
requirements**



**Work Stream
4: on Cross-
Border
dependencies**



**Work Stream
5: Digital
Service
Providers**

NIS Implementation

Work Streams 2/2



**Work Stream 6:
Cybersecurity
of Elections**



**Work Stream 7:
Large scale
cyber incidents
and crisis**



**Work Stream 8:
Sectoral
aspects
influencing the
implementation
of the Directive
(i.e. energy
sector)**



**Work Stream 9:
on Capacity
building**



**Work Stream
10: Synergies
between
incident
reporting
mechanisms
(i.e. GDPR,
eIDAS,
Telecom)**

Wider cybersecurity cooperation issues

Blueprint

**Resilience through crisis management
and rapid emergency response**

Blueprint – Coordinated Response to large scale incidents and crises



Blueprint activities:

- **Blueprint in PACE 2018**
- **NIS Cooperation Group Work Stream on Blueprint**
- **Blueprint Operational exercise [Blue OLEx 2019]/July 2019**
- **Standard Operating Procedures in 2019**
- **Cross-layer test of Blueprint in Cyber Europe 2020**

5G Security

COMMISSION RECOMMENDATION ON CYBERSECURITY OF 5G NETWORKS

COMMISSION RECOMMENDATION ON CYBERSECURITY OF 5G NETWORKS



12 March 2019 Report by the European Parliament.



22 March 2019 Conclusions by the European Council.



26 March 2019 Commission Recommendation on the cybersecurity of 5G networks



July 2019 Member States national risk assessments



9 October 2019 EU coordinated risk assessment of 5G networks security.



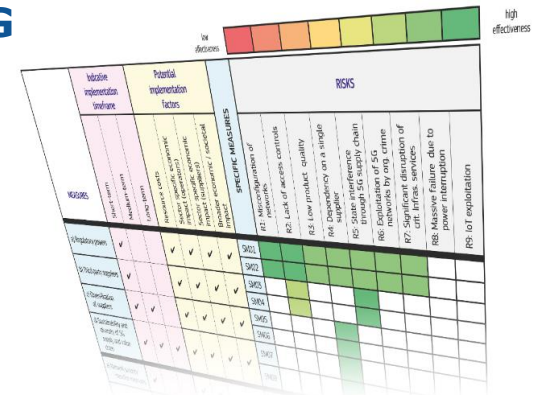
21 November 2019 ENISA report on threats relating to 5G networks.



29 January 2020 EU toolbox of mitigation measures and Commission Communication on the implementation of the EU toolbox.

EU toolbox for 5G networks – Jan. 2020

- Provides risk mitigation plans for all 9 risks identified in the EU risk assessment (incl. risk of interference from non-EU state or state-backed actors through 5G supply chain).
- Proposes a combination of 8 strategic and 11 technical measures to mitigate the risks, and 10 corresponding supporting actions to reinforce their effectiveness.
- Shows strong resolve of Member States to jointly respond to 5G cybersecurity challenges
- Lists both MS and EU measures and clear next steps at EU and national levels
- Strengthens security requirements for mobile operators
- Foresees the risk profile of suppliers, with relevant restrictions for suppliers considered to be high risk - including necessary exclusions.
- Promotes multi-vendor strategies for operators



		Measures		Risks	
		Strategic measures	Technical measures	Supporting actions	
R1	Interference from non-EU state or state-backed actors through 5G supply chain	✓	✓	✓	✓
	Interference from non-EU state or state-backed actors through 5G supply chain	✓	✓	✓	✓
R2	Low product quality	✓	✓	✓	✓
	Low product quality	✓	✓	✓	✓
R3	Dependency on a single supplier	✓	✓	✓	✓
	Dependency on a single supplier	✓	✓	✓	✓
R4	State-backed actors	✓	✓	✓	✓
	State-backed actors	✓	✓	✓	✓
R5	Significant disruption of networks by eng. centre	✓	✓	✓	✓
	Significant disruption of networks by eng. centre	✓	✓	✓	✓
R6	Significant disruption of 5G networks by eng. centre	✓	✓	✓	✓
	Significant disruption of 5G networks by eng. centre	✓	✓	✓	✓
R7	Significant disruption of 5G networks by eng. centre	✓	✓	✓	✓
	Significant disruption of 5G networks by eng. centre	✓	✓	✓	✓
R8	Massive failure due to power interruption	✓	✓	✓	✓
	Massive failure due to power interruption	✓	✓	✓	✓
R9	IoT exploitation	✓	✓	✓	✓
	IoT exploitation	✓	✓	✓	✓

Communication – Jan. 2020

- **Integral part of the Commission's comprehensive European digital strategy.**
- **COM to undertake measures to ensure implementation in the areas under its competence (COM(2020)50):**
 - **Telecoms & cybersecurity rules –*Telecoms Code***
 - **Standardisation – *Standards bodies***
 - **Certification – *5G certification schemes***
 - **FDI – *screening & mapping 5G value chain / scrutinizing 5G investments***
 - **Trade defense – *market developments & protect EU actors***
 - **Competition rules – *contractual or technical 'lock-in' supplier situations***
 - **EU funding – *compliance security requirements / innovation programmes***
 - **Public procurement – *cybersecurity requirements for 5G contracts***
 - **Industrial development & deployment – *e.g. IPCEI (Common European Projects of European Interest)***



A cybersecurity competence network with a European Cybersecurity Research and Competence Centre

**Reinforcing EU's cybersecurity technologic
capabilities and skills**

The situation today

Key cybersecurity technologies – where does the EU stand



The EU represents 26% of the global cybersecurity market

CYBERSECURITY PRODUCTS AND SOLUTIONS

Up to 30% of the European demand is met by companies headquartered outside the EU.

Europe is the location for the corporate headquarters of only 14% of the top 500 global Cybersecurity providers, compared to 75% for the Americas, 7% for Israel and 4% for Asia.

A wealth of cybersecurity knowledge in Europe



*More than 660 expertise centres
registered in the mapping of
cybersecurity centres of expertise*

ECSO has +/- 240 members



EU pilots helping to prepare the European Cybersecurity Competence Network

More than **€63.5 million** invested in **4 projects**



 Partners: **46**

 EU Member States involved: **14**

Key words

SME & startup ecosystem
Ecosystem for education
Socio-economic aspects of security
Virtual labs and services
Threat Intelligence for Europe
DDoS Clearing House for Europe
AI for cybersecurity
Post-Quantum cryptography



 Partners: **43**

 EU Member States involved: **20**

Key words

Cybersecurity for citizens
Application cases
Research Governance
Cyber Range
Cybersecurity certification
Training in security



 Partners: **30**

 EU Member States involved: **15**

Key words

Network of Cybersecurity centres
Cyber Range
Cybersecurity demonstration cases
Cyber-skills Framework
Cybersecurity certification
Cybersecurity early warning



 Partners: **44**

 EU Member States involved: **14**

Key words

Research Governance
Cybersecurity skills
Cybersecurity certification
Community engagement
International cooperation
Strategic Autonomy



The proposal in a nutshell

European Cybersecurity Technology & Innovation Ecosystem



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

The Competence Centre – what will it do?

**Facilitate and help
coordinate the work of
the Network**

**Implement cybersecurity
parts of Digital Europe
and Horizon Europe
Programmes**

**Enhance cybersecurity
capabilities, knowledge
and infrastructures**

**Contribute to the wide
deployment of state-of-the-
art products and solutions;
support SMEs**

**Contribute to reducing
cybersecurity skills gaps**

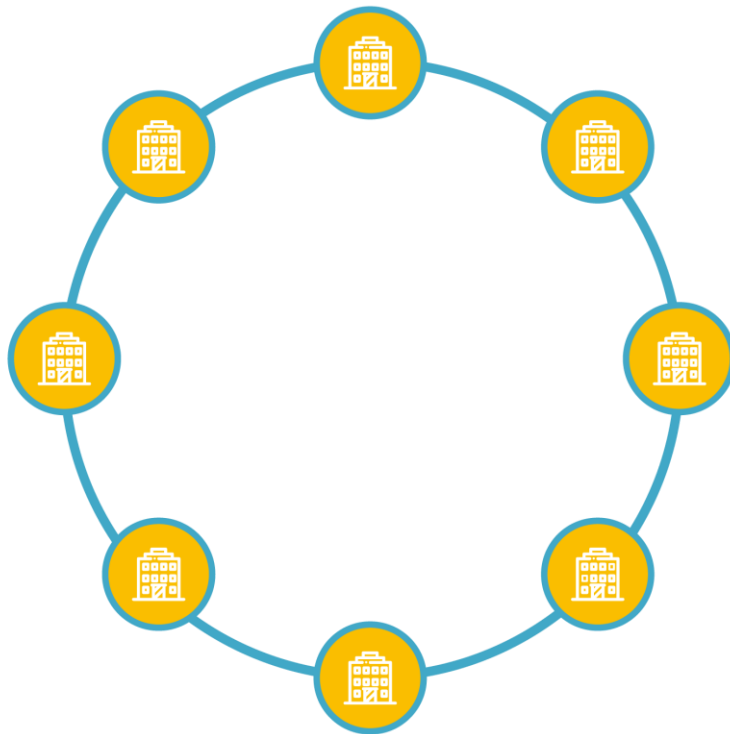
**Support cybersecurity
research
and development**

**Enhance cooperation
between the civilian and
defence spheres with regard
to dual use technologies**

**Enhance synergies in
relation to the European
Defence Fund**



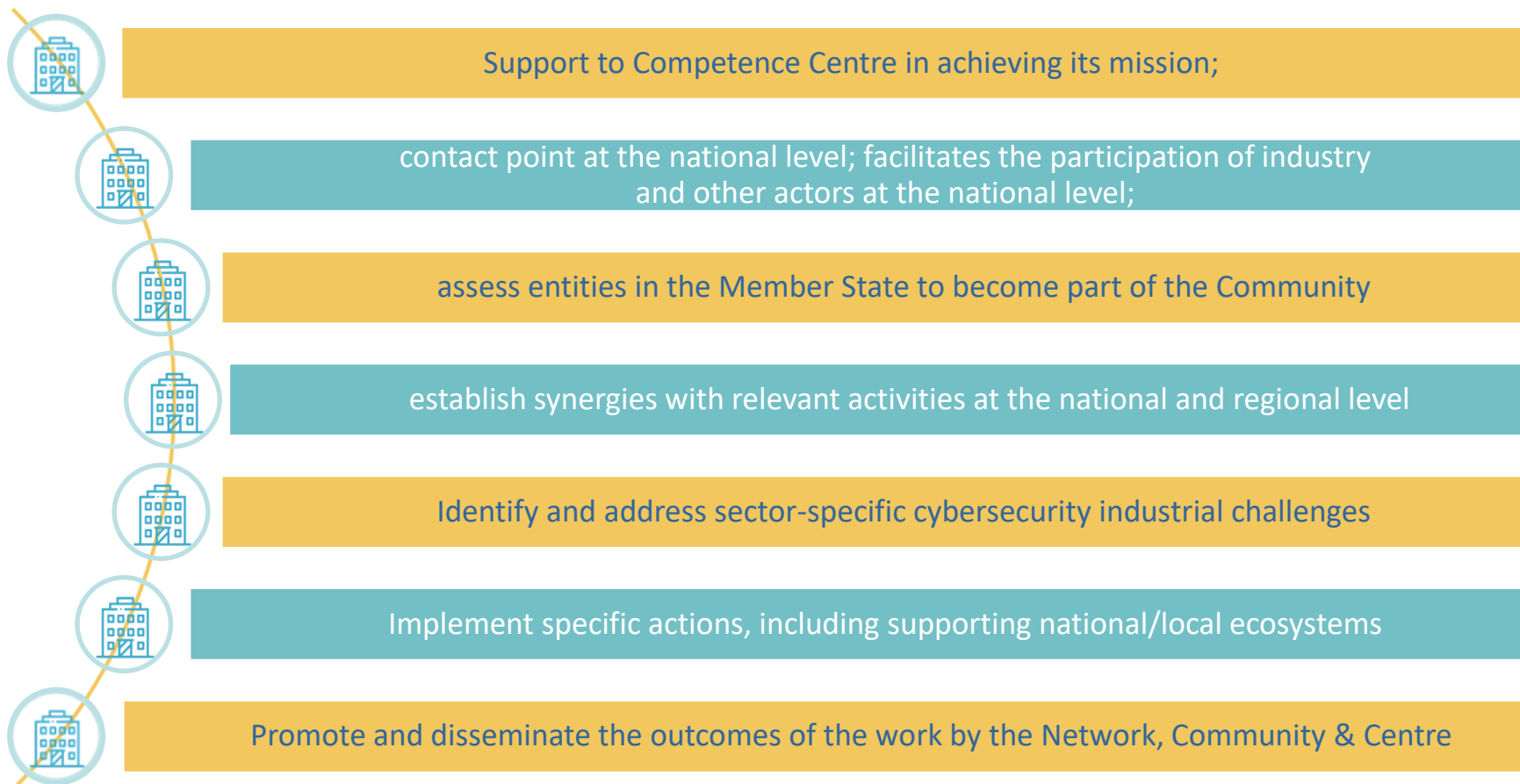
Network of National Coordination Centres



National Coordination Centres:

- Nominated by Member States & notified to the Commission
- Possess or have access to technological expertise in cybersecurity
- Can effectively engage and coordinate with industry, academia and the public sector
- Can receive direct grants
- Can provide financial support to third parties

Tasks of the National Coordination Centres



Cybersecurity Competence Community



Academic and research organisations



Industry (demand and supply)



Public Authorities



Other stakeholders



Union bodies with relevant experience



Relevant Associations

An open and diverse group of actors involved in cybersecurity technology

Expertise in research, industrial development or training and education required

Assessment done by the Member State where the entity is established and then accredited by the Competence Centre

Only entities established within the Union may be accredited

Cybersecurity Competence Community



Academic and research
organisations



Industry
(demand and supply)



Public Authorities



Other stakeholders



Union bodies with
relevant experience



Relevant Associations

**Support the Centre and the
Network in achieving the mission
and objectives**

**Enhance and disseminate
cybersecurity expertise across the
Union**

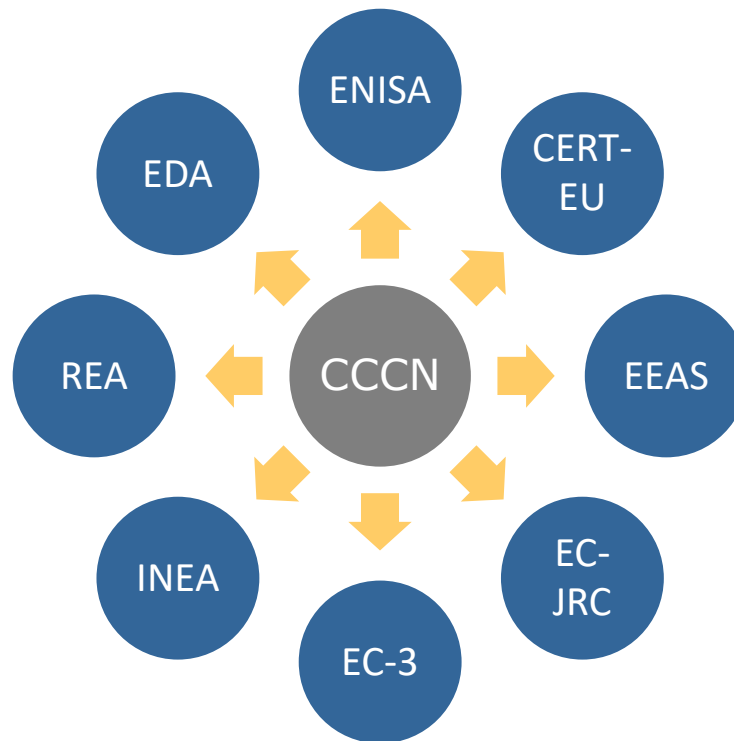
**Participate in activities promoted
by the Network and the Centre**

**Participate in the working groups
on specific activities**

**Promote the outcomes of specific
projects**

Coordination and Cooperation

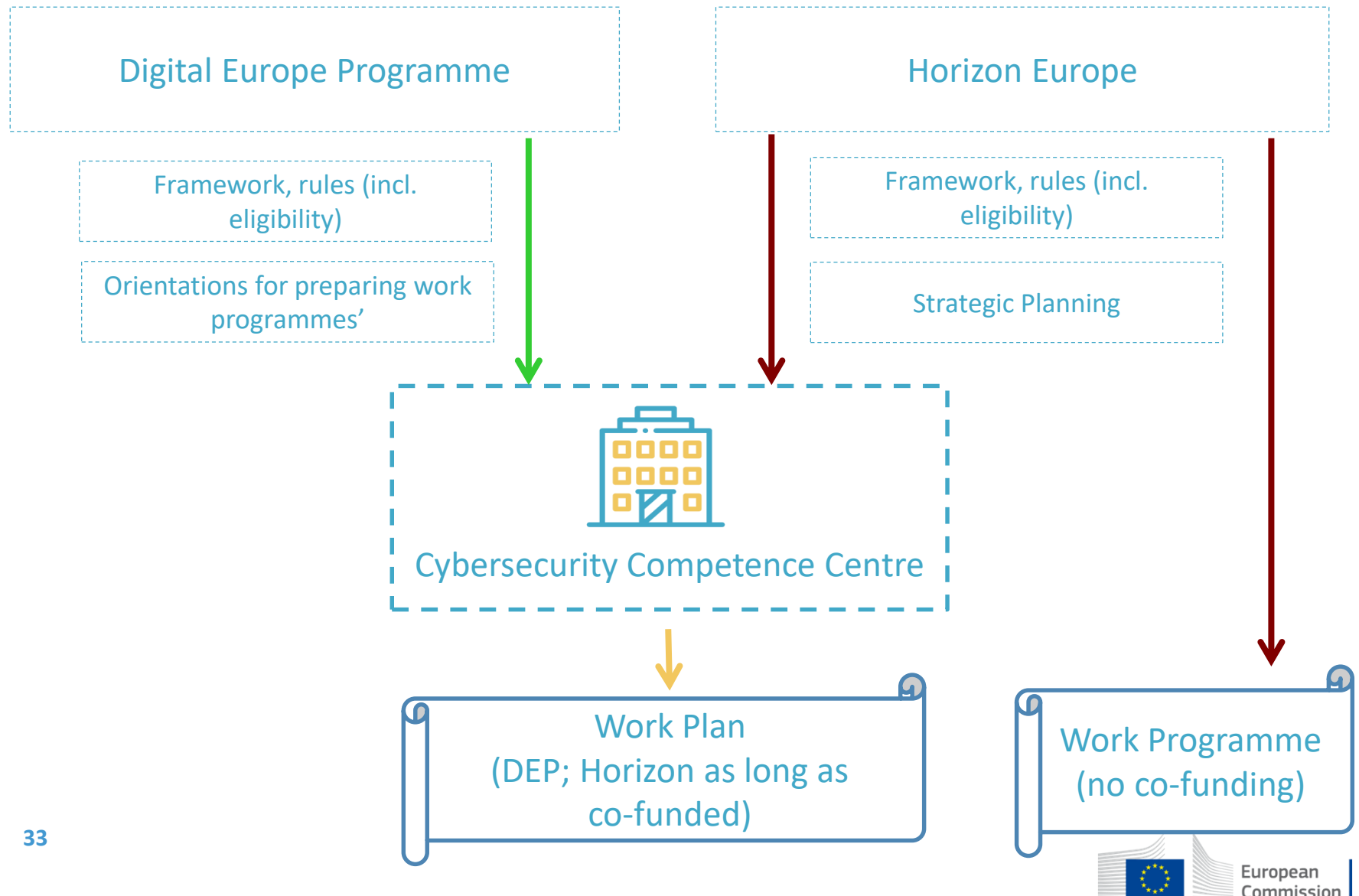
working arrangements to be concluded with relevant Union institutions, bodies, offices and agencies





Financing of the initiative

Relationship between programmes and Competence Centre



Why set up a co-financing mechanism for cybersecurity?

Going beyond the status quo

- Not only support scientific excellence but develop and deploy capabilities
- Support skills
- achieve industrial leadership

Align strategies around an agenda agreed with all relevant stakeholders;

Coordinate the investments which are taking place

Different types of projects

- Large-scale federating projects/infrastructures
- Support capacity building (public authorities, SMEs, operators of essential services); achieve economies of scale
- Research and innovation projects as known from Horizon2020

Pooling resources where relevant



Funding priorities – EC planning

Horizon 2020 upcoming cybersecurity topics

- SU-DS02-2020: Intelligent security and privacy management. (RIA/IA, 38.00 MEUR
27/08/2020)
- SU-DS03-2019-2020: Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises. (IA, 10.80 MEUR 27/08/2020)
- SU-DS04-2018-2020: Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches. (IA, 20.00 MEUR
27/08/2020)
- SU-INFRA01-2018-2019-2020: Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe. (IA, 20.70 MEUR
27/08/2020)
- SU-AI-2020: Artificial Intelligence and security: providing a balanced assessment of opportunities and challenges for Law Enforcement in Europe (IA, CSA 20.00 MEUR
27/08/2020)^a

DIGITAL EUROPE - initial funding priorities

- **Support to the network of National Coordination Centres;**
- **Key capacity building: the cybersecurity shield**
Deploying a quantum-secured public communication infrastructure (terrestrial segment) with the aim at deploying Quantum Key Distribution (QKD) in various large-scale networks;
Deploying through cyber ranges, with Member States and industry, a European cyber threat information network;
- **Certification scheme(s)**
Support certification capacities
Support SMEs to certify their products
Provide certification testbed;
- **Widening the deployment of cybersecurity tools**
Support for faster validation and market take-up of innovative cyber security solutions by businesses and public buyers;
- **Supporting the NIS Directive implementation**
Strengthening the activities started under the current CEF Telecom programme (national authorities, CSIRTs, OES, DSP, ...)

HORIZON EUROPE - initial funding priorities

- Resilient infrastructures and interconnected systems
- Security quantification and certification
- Hardware, software and supply chain security
- Advanced cryptography
- Securing disruptive technologies, e.g. AI, big data
- Security, privacy, and ethics

Trust in a Digital Society

