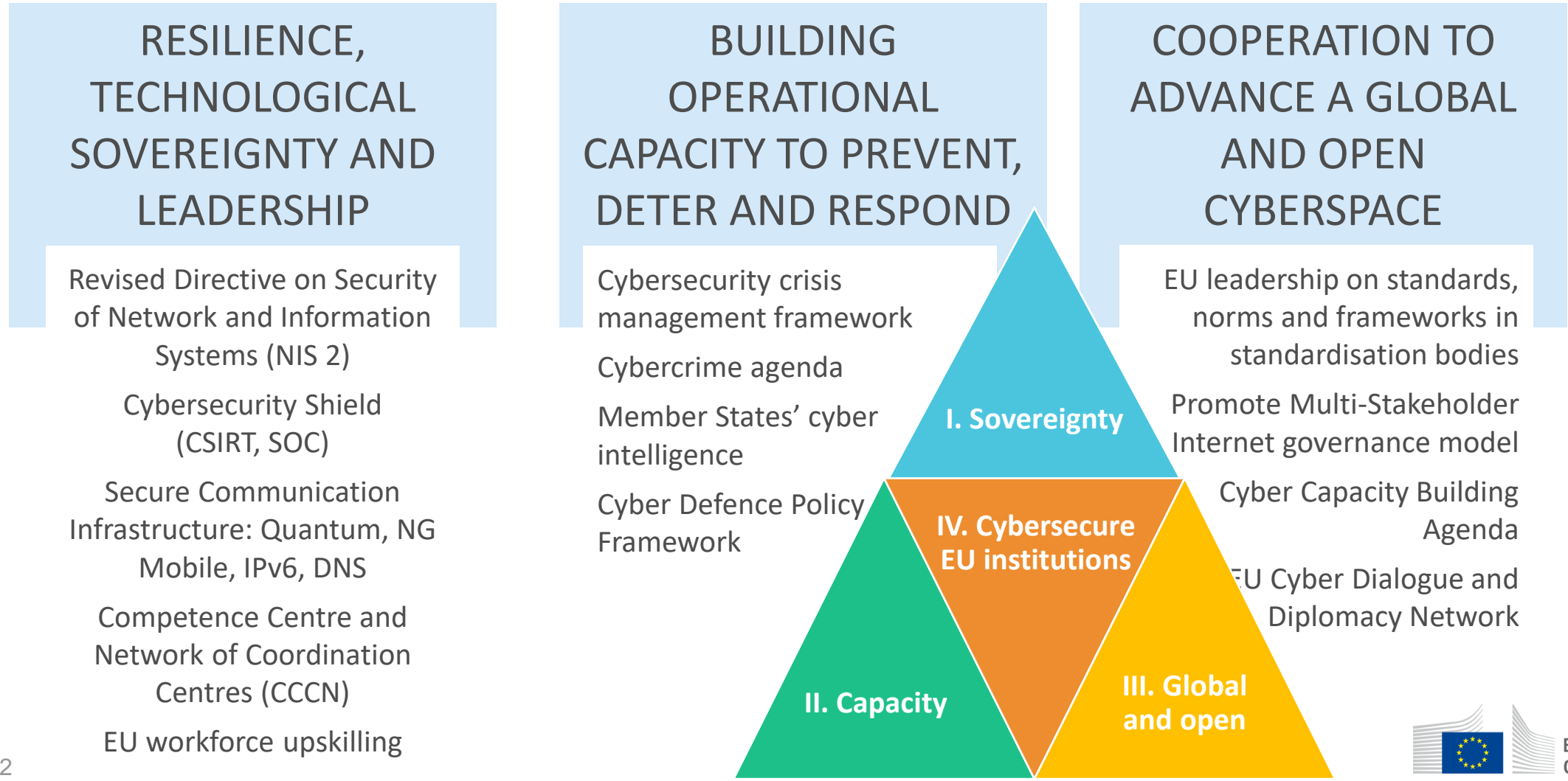# EU Strategy and Investments in Cybersecurity

ENISA Cybersecurity Market Analysis Conference

24 November 2022

Ioannis Askoxylakis

The EU's Cybersecurity Strategy for the Digital Decade (16.12.2020); 3 instruments (regulatory, investment, policy initiatives) 3 to three pillars

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

I. Sovereignty

IV. Cybersecure EU institutions

II. Capacity

III. Global and open

European Commission

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

- (…)

European Commission

A EUROPEAN CYBERSECURITY TECHNOLOGY & INNOVATION ECOSYSTEM

EU Funding, Capacity-building, Community-building

European Commission

# EU Cybersecurity Competence Centre and Network

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 (NCCs):

➢ Nominated by Member States as the national contact point
➢ Objective: national capacity building and link with existing initiatives
➢ May receive funding, may pass on financial support
➢ One NCC per Member State

Competence Community:

➢ A large, open, and diverse group of cybersecurity stakeholders from research and the private and public sectors
➢ Provides input to the activities of the competence centre to the work programmes
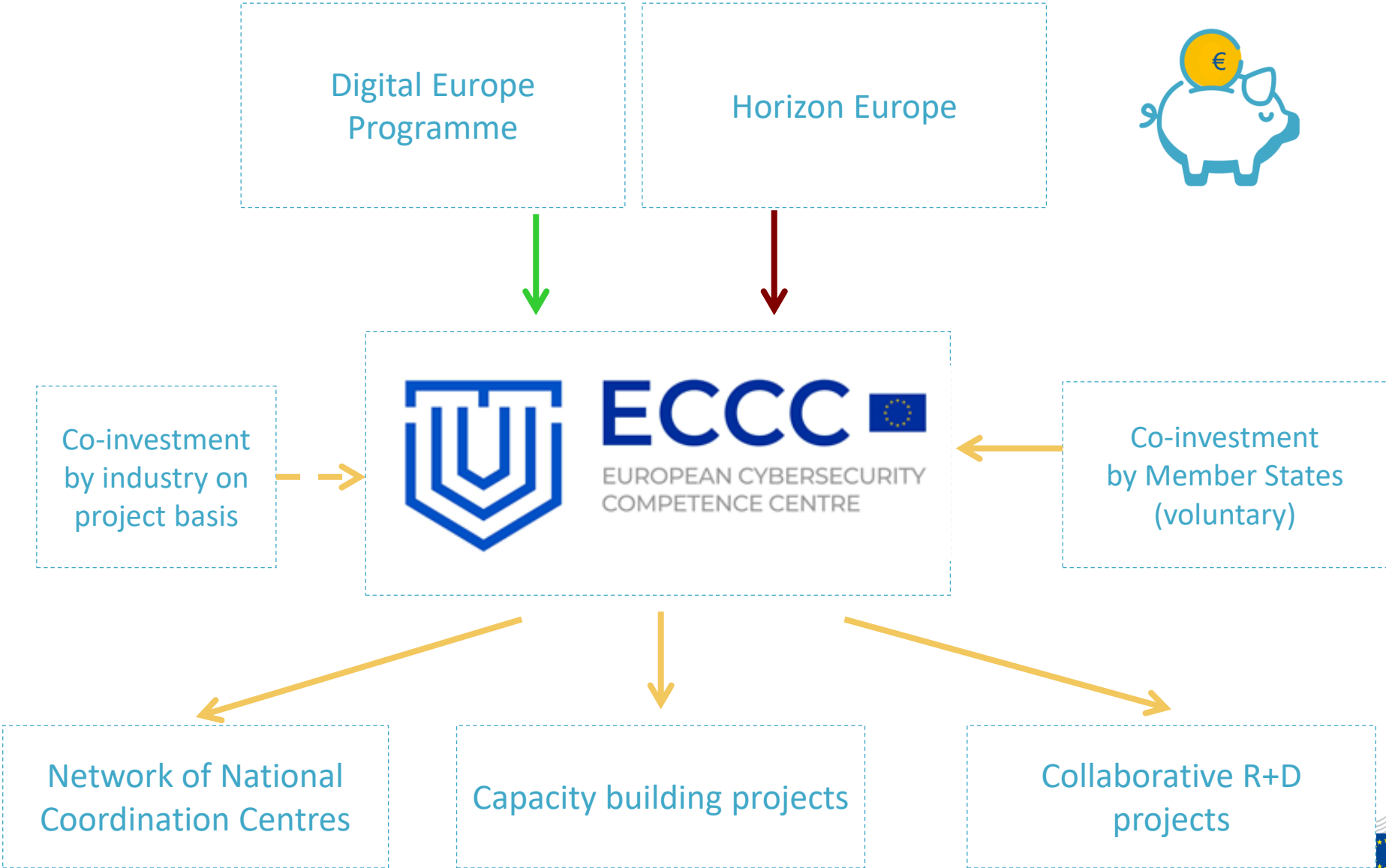
European Commission
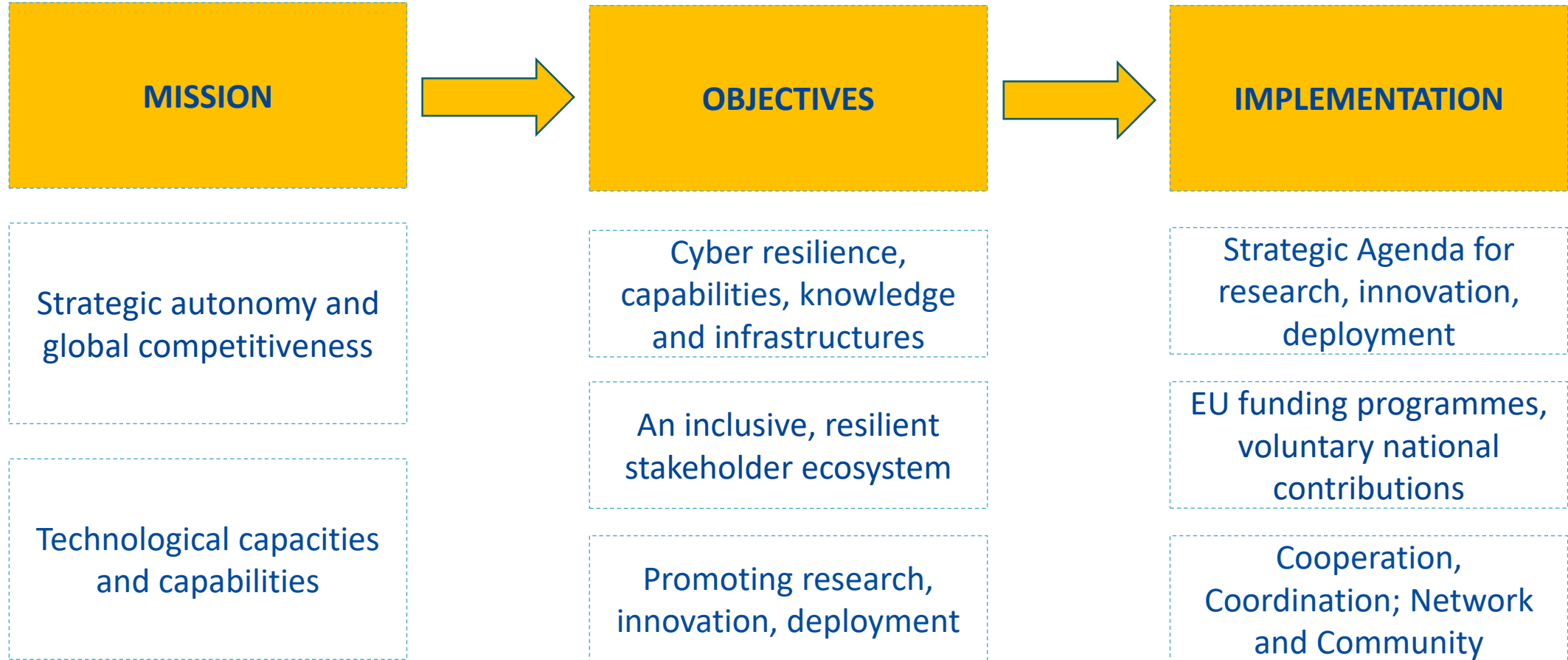
Network of National Coordination Centres

➢ One NCC per Member State, nomainated by the Member State

➢ May receive EU funding

➢ May pass on EU funding

➢ Objective: national capacity building and link with existing initiatives

➢ Contributes to strategic tasks

➢ Promotes participation in cross-border projects and in cybersecurity action

➢ Provides technical assistance

➢ Coordinates the national, regional and local levels

➢ Asses requests by entities in the Member States

➢ Promotes cybersecurity educational programmes

➢ Advocates involvement of relevant entities
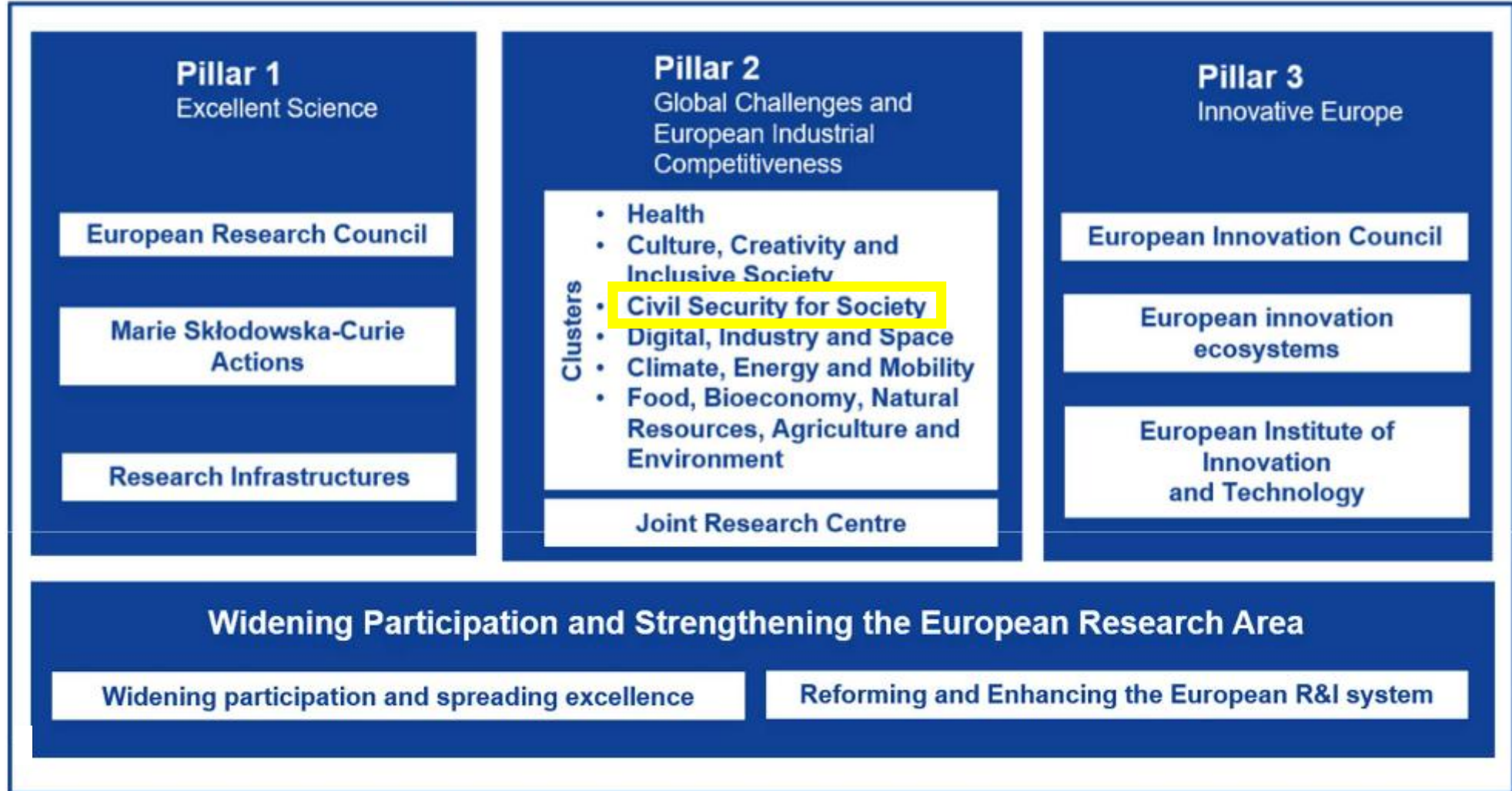
European Commission

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 which acts cross-sectoral and cross-department

➢ Management of the Community has been prepared through the pilots CONCORDIA, ECHO, SPARTA and CyberSec4Europe

➢ The Centre, Network and Community should help to advance and disseminate the latest cybersecurity products and services

➢ Exchanges with the Centre on developments in cybersecurity

➢ Provides input to the activities of the competence centre to the multiannual work programme and to the annual work programme

➢ Splits up into working groups for regular dialogue

➢ Supports stakeholders at their request, public-private coordination

European Commission

2021-2027 proposed EU cybersecurity funding sources

Horizon Europe 2022

Horizon Europe - Structure

Digital Europe programme structure

ACCELERATING THE BEST USE OF DIGITAL TECHNOLOGIES

Digital Innovation Hubs

High impact deployments

BUILDING ESSENTIAL DIGITAL CAPACITIES

High Performance Computing

Artificial Intelligence

Cybersecurity

Advanced Digital Skills

European Commission
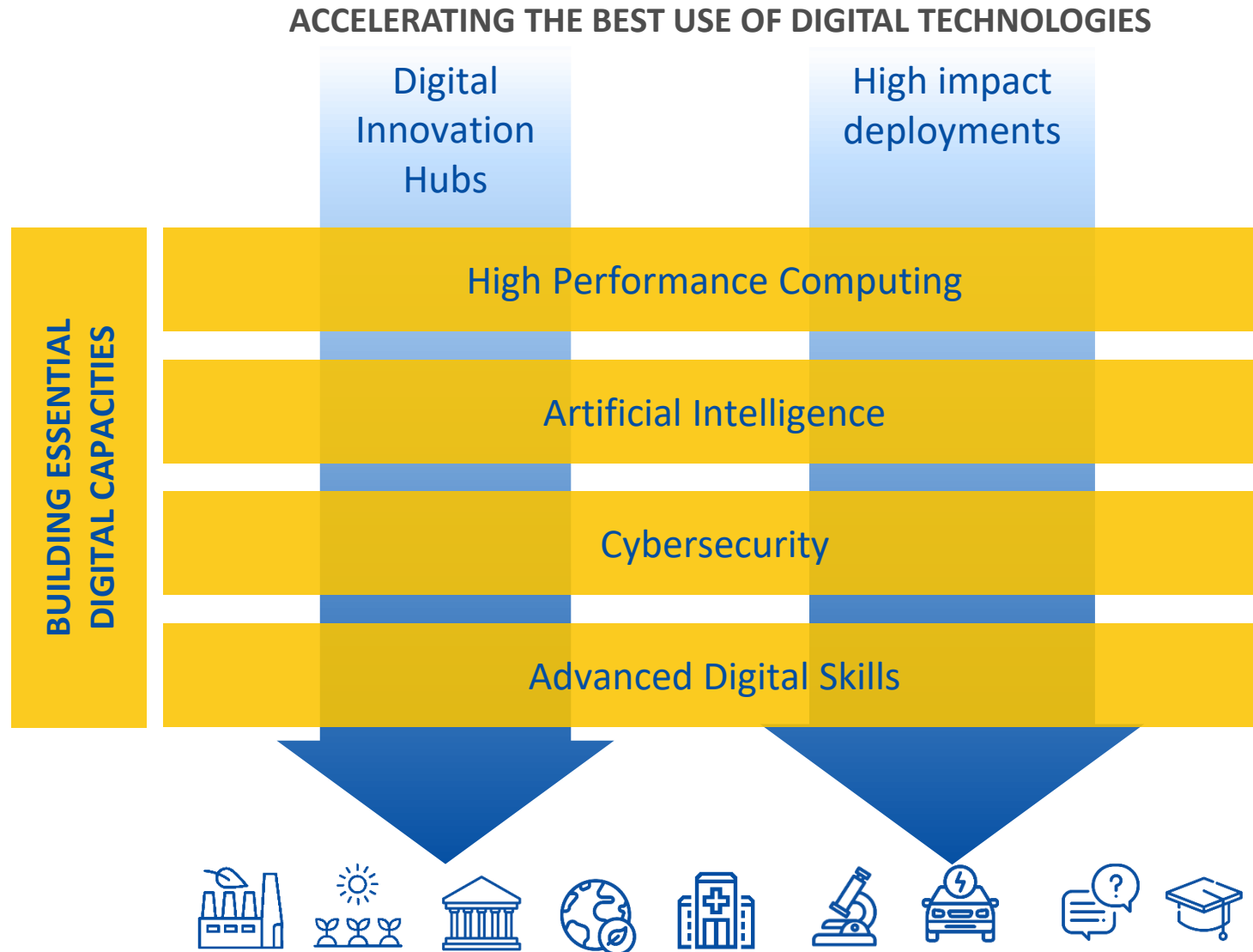
Horizon Europe – Work Programme 2021-22 (135m EUR)

Cybersecurity Topics 2022
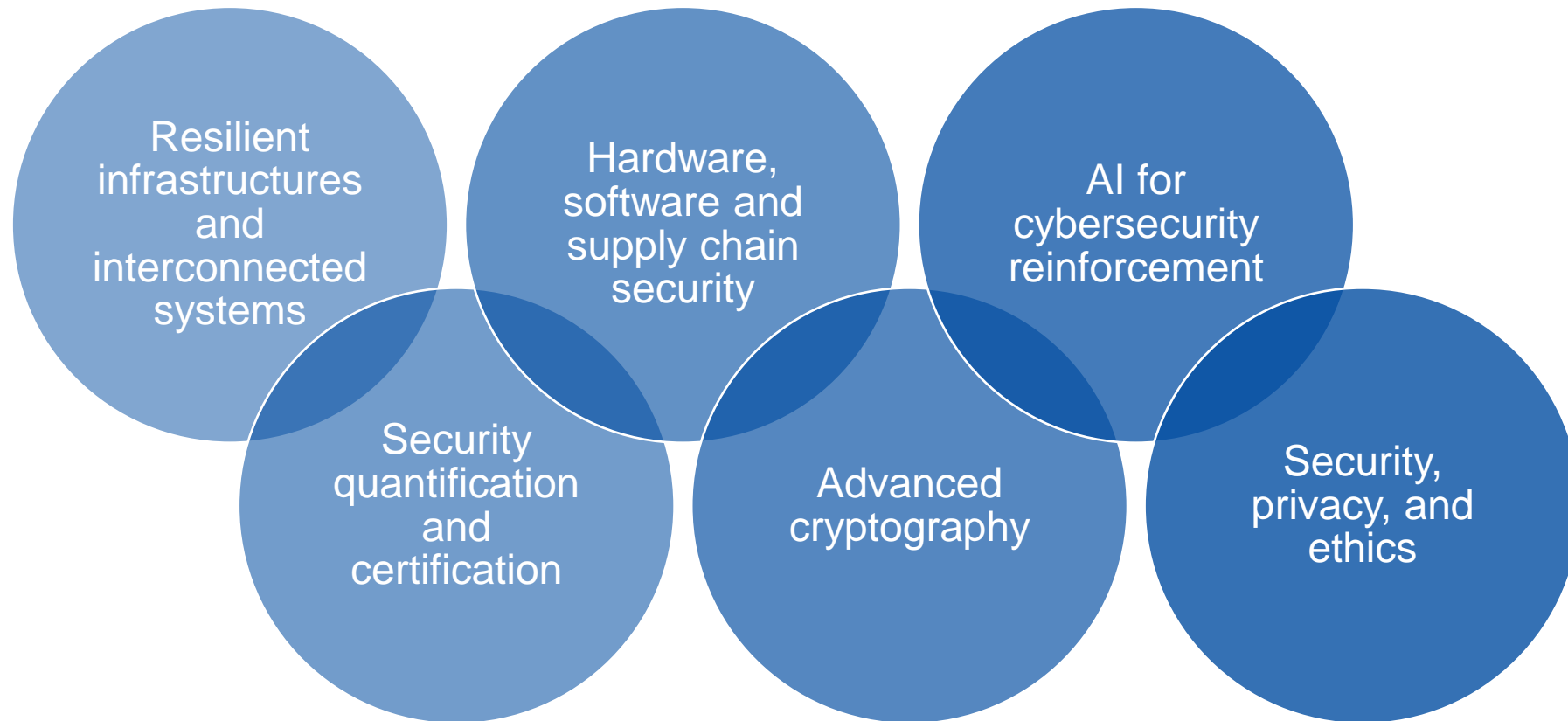
Resilient digital infrastructures and interconnected systems

HORIZON-CL3-2022-CS-01-01: Improved monitoring of threats, intrusion detection and response in complex and heterogeneous digital systems and infrastructures

Hardware, software and supply chain security

HORIZON-CL3-2022-CS-01-02: Trustworthy methodologies, tools and data security "by design" for dynamic testing of potentially vulnerable, insecure hardware and software components

Cybersecurity and disruptive technologies

HORIZON-CL3-2022-CS-01-03: Transition towards Quantum-Resistant Cryptography

Smart and quantifiable security assurance and certification shared across Europe

HORIZON-CL3-2022-CS-01-04: Development and validation of processes and tools used for agile certification of ICT products, ICT services and ICT processes

For more information:

HE Programme 2021/22 - 6. Civil Security for Society

General Annexes of the WP
Standard application form (RIAs/IAs)

Participant Portal

For questions contact

us: CNECT-H1-EVALUATIONS@ec.europa.eu

Digital Europe work programme 2021-22

- **European Cyber-shield (147m EUR)**
    - EU cybersecurity resilience, coordination and cybersecurity ranges
    - Capacity building of Security Operation Centres (SOCs)
    - Secure 5G and other strategic digital infrastructures and technology
    - Uptake of innovative cybersecurity solutions in SMEs
    - Support to the health sector cybersecurity
- **Support to implementation of relevant EU Legislation (83m EUR)**
    - Network of National Coordination Centres
    - Cybersecurity Community support
    - NIS Directive implementation and national cybersecurity strategies
    - Testing and certification capabilities
- **Secure quantum communication infrastructure (174m EUR)**
- **Skills (incl. Cyber – 166m EUR)**

Topics and deadlines upcoming topics

Topic	Budget	Opening	Deadline
Network of National Coordination Centres	€ 55M (total)		
EU cybersecurity resilience, coordination and cybersecurity ranges	€ 15M		
Capacity building of Security Operation Centres (SOCs)	€ 72,5M		
Secure 5G and other strategic digital infrastructures and technology	€ 10M	29 September	24 January 2023
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

Thank you

European Commission