EUROPEAN UNION AGENCY
FOR CYBERSECURITY

THE EU CYBERSECURITY STRATEGY FOR A QUANTUM-SAFE FUTURE

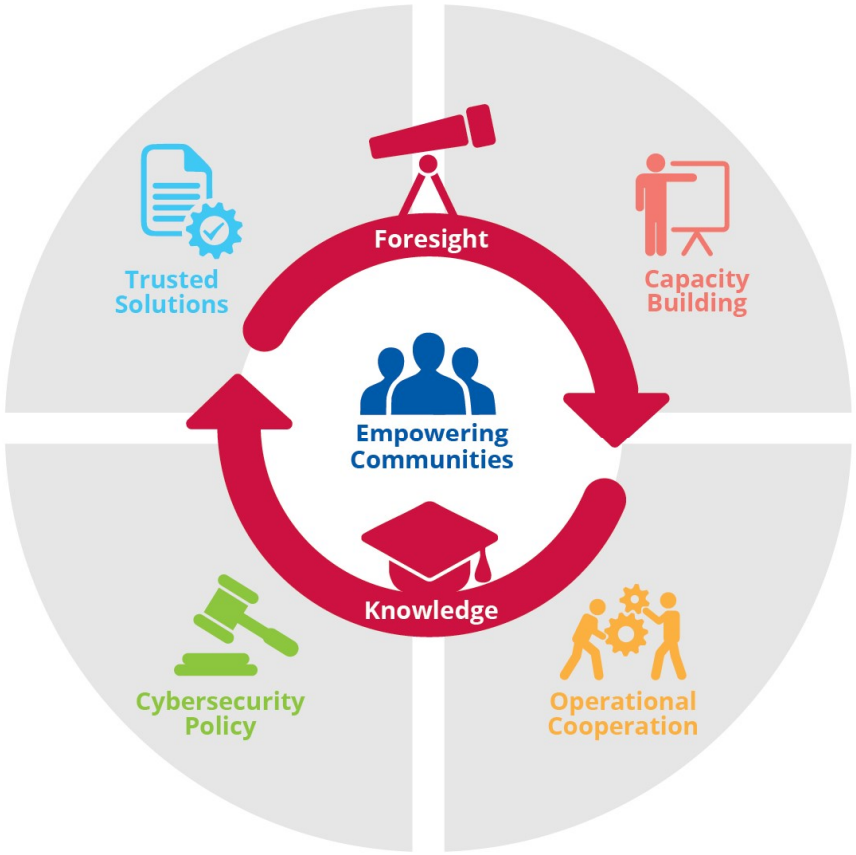
ETSI - IQC QUANTUM-SAFE CRYPTOGRAPHY WORKSHOP

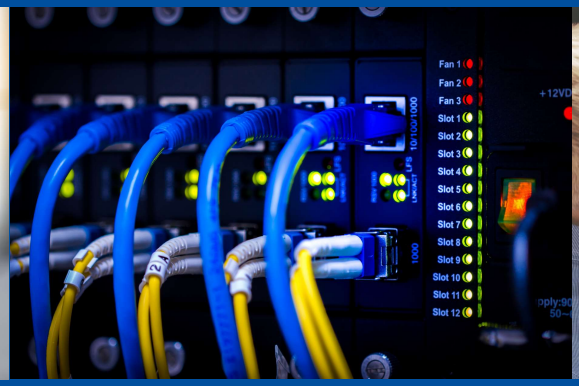
Marco Barros Lourenco
RESEARCH AND INNOVATION LEAD

13 | 02 | 2023

ABOUT ENISA

THE AGENCY


Foresight
Capacity Building
Trusted Solutions
Empowering Communities
Knowledge
Cybersecurity Policy
Operational Cooperation


EU STRATEGY FOR CYBERSECURITY

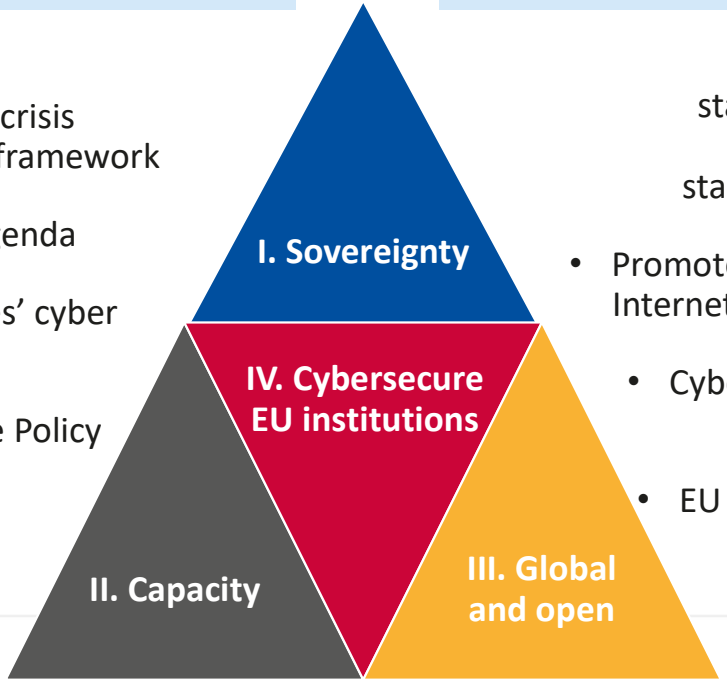
THE EU'S CYBERSECURITY STRATEGY FOR THE DIGITAL DECADE THREE INSTRUMENTS (REGULATORY, INVESTMENT, POLICY INITIATIVES) AND THREE PILLARS

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

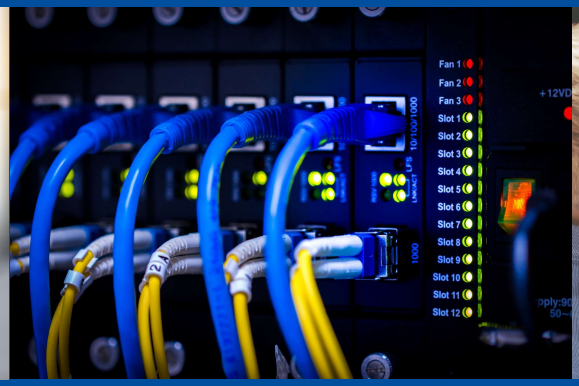


COOPERATION TO ADVANCE A GLOBAL AND OPEN CYBERSPACE

- 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

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
- (…)



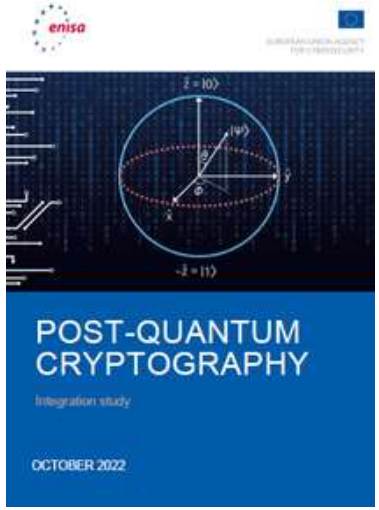
EU ACTION ON QUANTUM COMPUTING AND PQC

EU INITIATIVES

QUANTUM FLAGSHIP

The Quantum Technologies Flagship is a long-term research and innovation initiative that aims to put Europe at the forefront of the second quantum revolution.

SPARTA

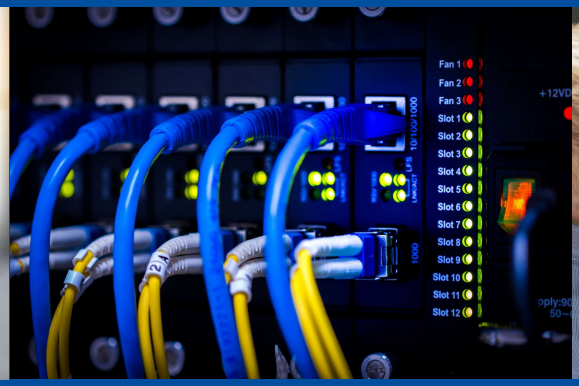


Current state of affairs on the standardization process of Post-Quantum Cryptography (PQC). It presents the 5 main families of PQ algorithms; viz. code-based, isogeny-based, hash-based, lattice-based and multivariate-based

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

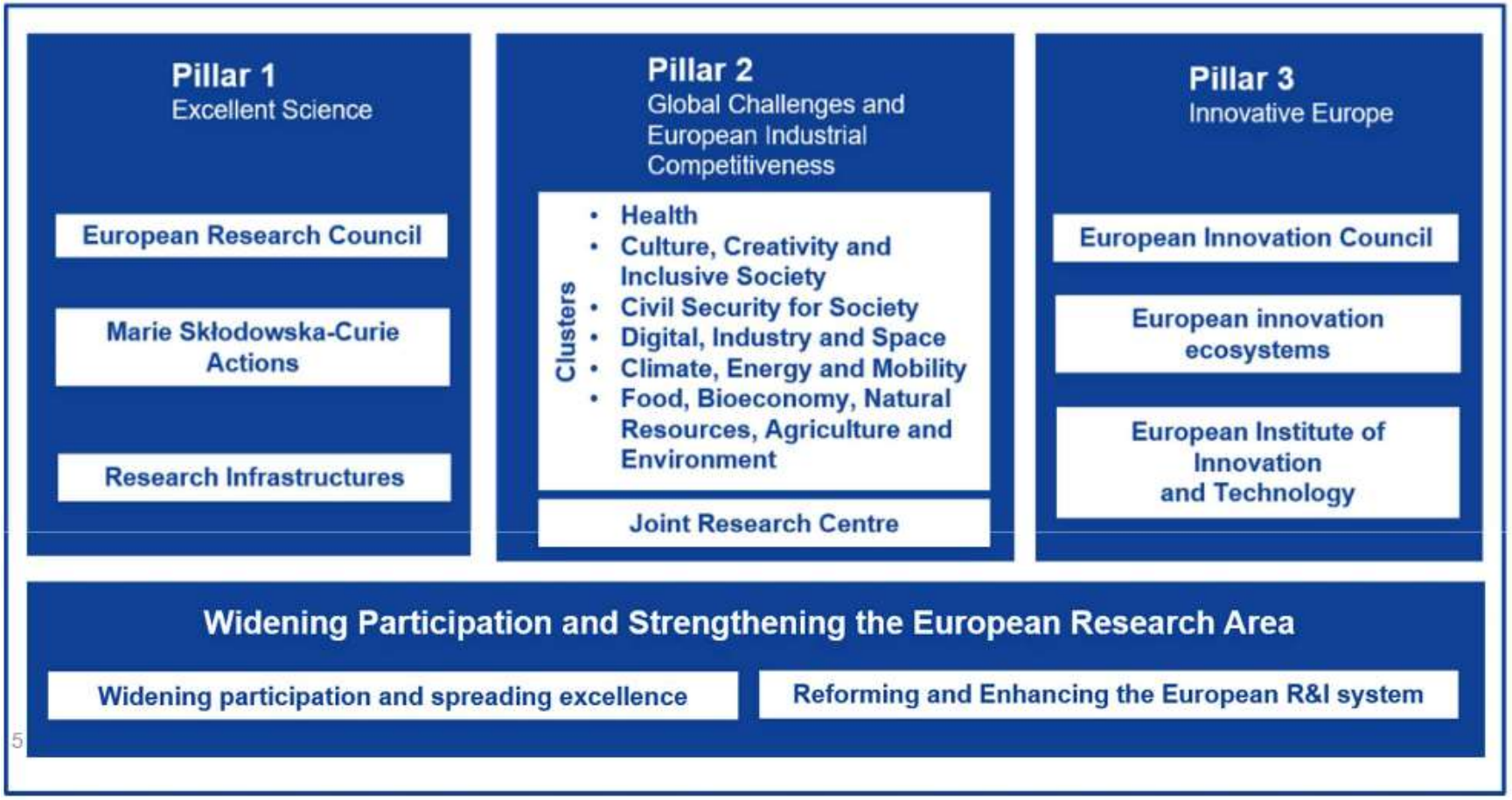
Cyber Security for Europe

ECHO
European network of Cybersecurity centres and competence Hub for innovation and Operations

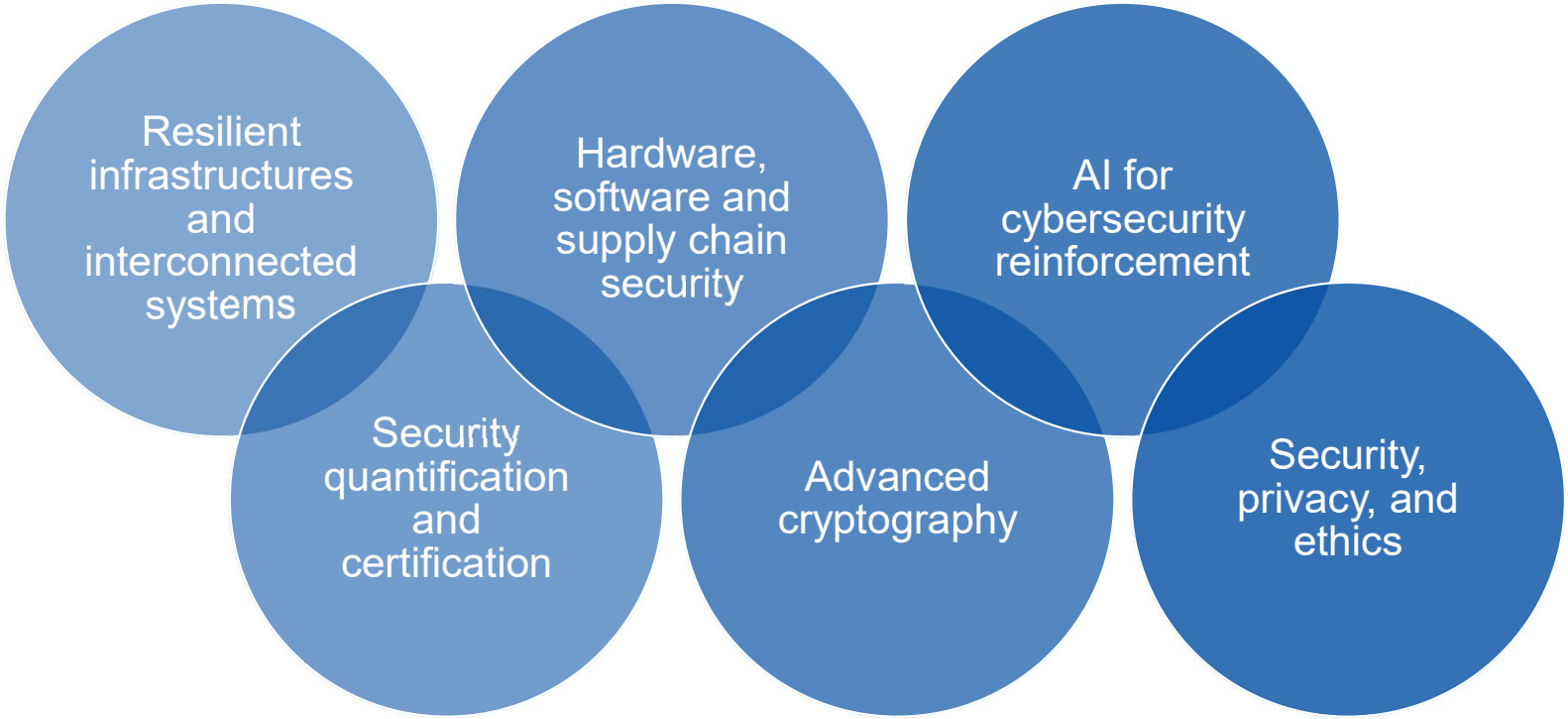




HORIZON EUROPE PROGRAMME

HORIZON EUROPE STRUCTURE



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

CYBERSECURITY TOPICS 2022

For more information:

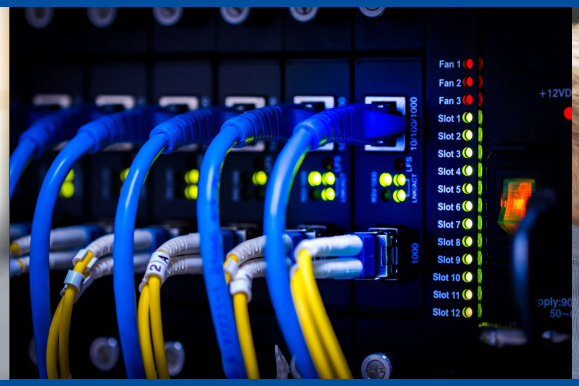
HE Programme 2021/22 - 6. Civil Security for Society

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

Participant Portal

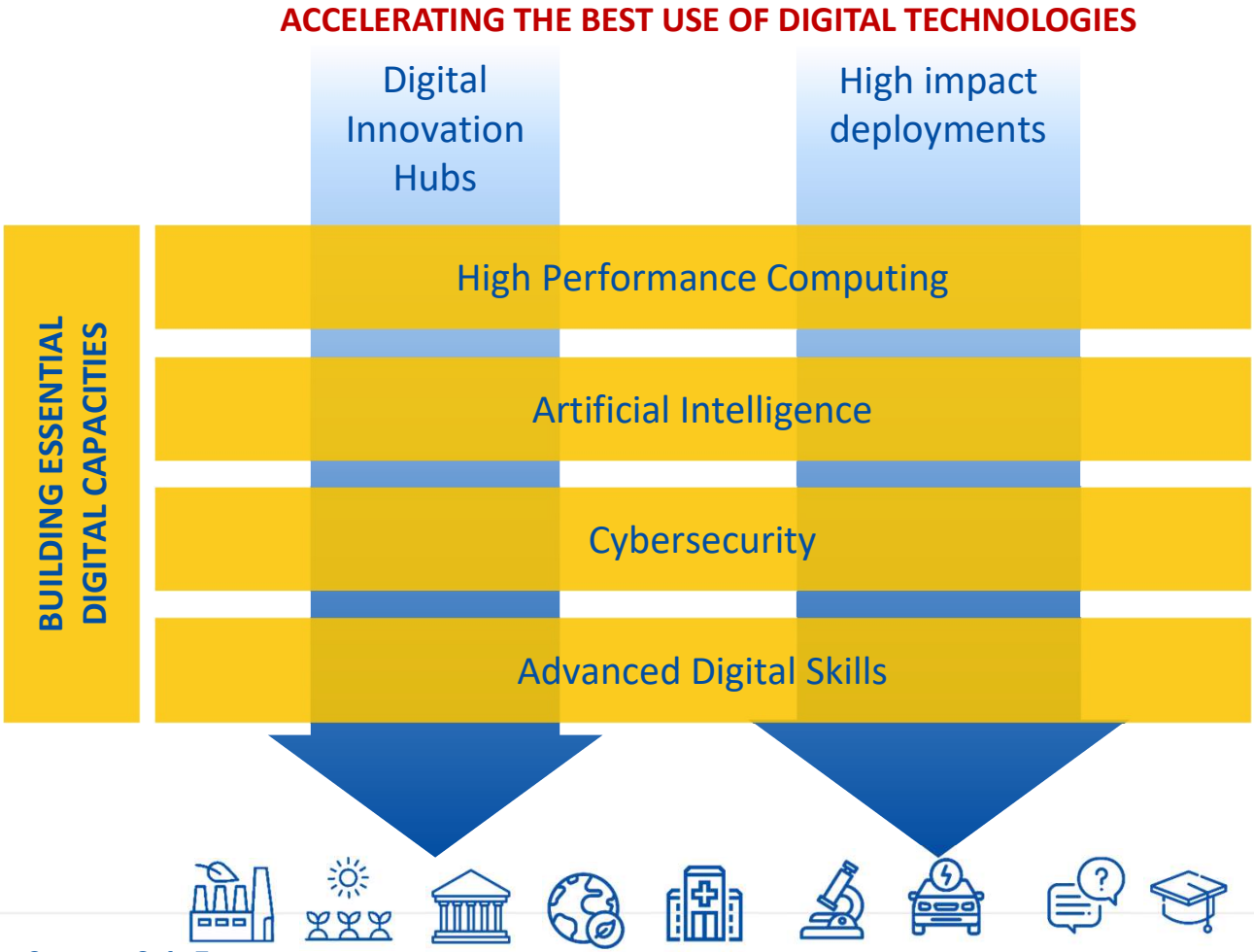
For questions contact

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



DIGITAL EUROPE PROGRAMME

DIGITAL EUROPE PROGRAMME STRUCTURE



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)**

USEFUL LINKS

- Digital Europe Programme website
- Digital Europe Programme Regulation
- Funding & tender opportunities portal

A EUROPEAN CYBERSECURITY TECHNOLOGY & INNOVATION ECOSYSTEM

EU FUNDING, CAPACITY-BUILDING, COMMUNITY-BUILDING

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.

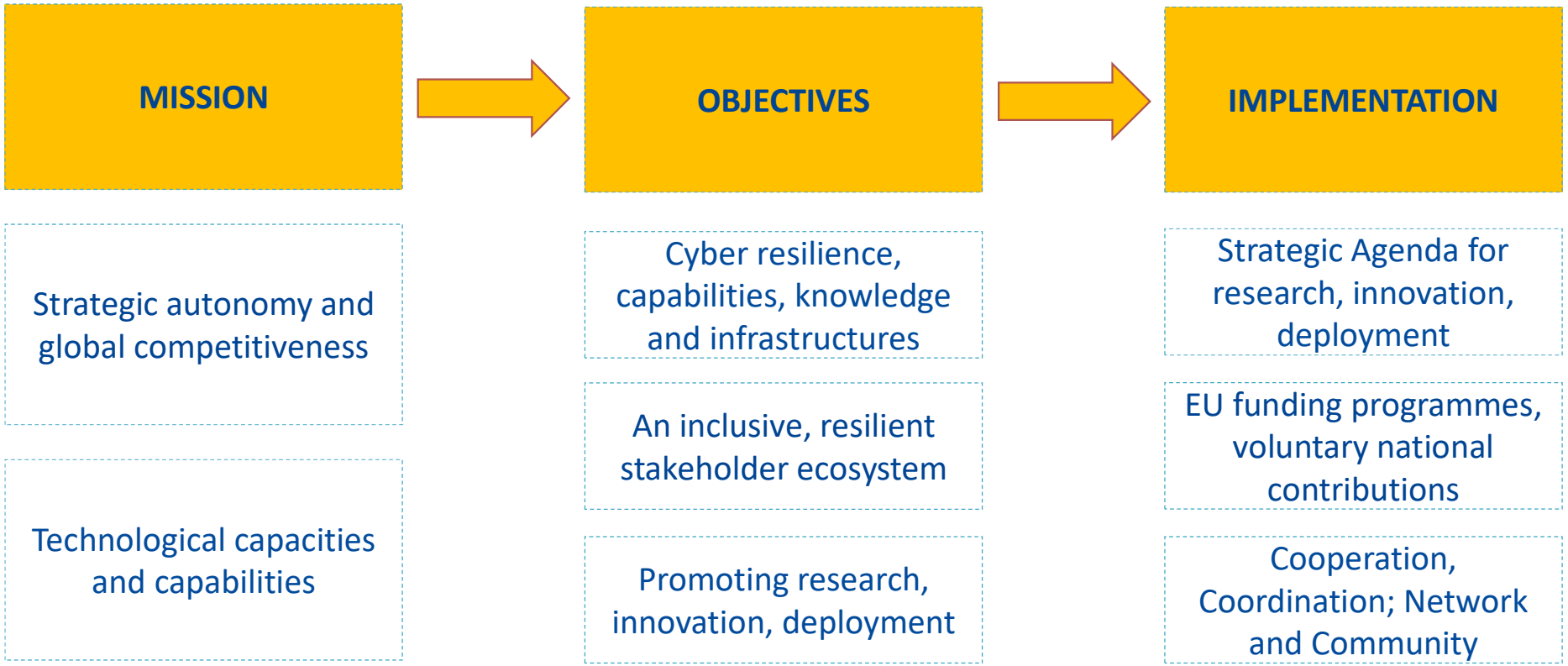
Network of National Coordination Centres (NCCs):

- 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

EU CYBERSECURITY COMPETENCE CENTRE AND NETWORK



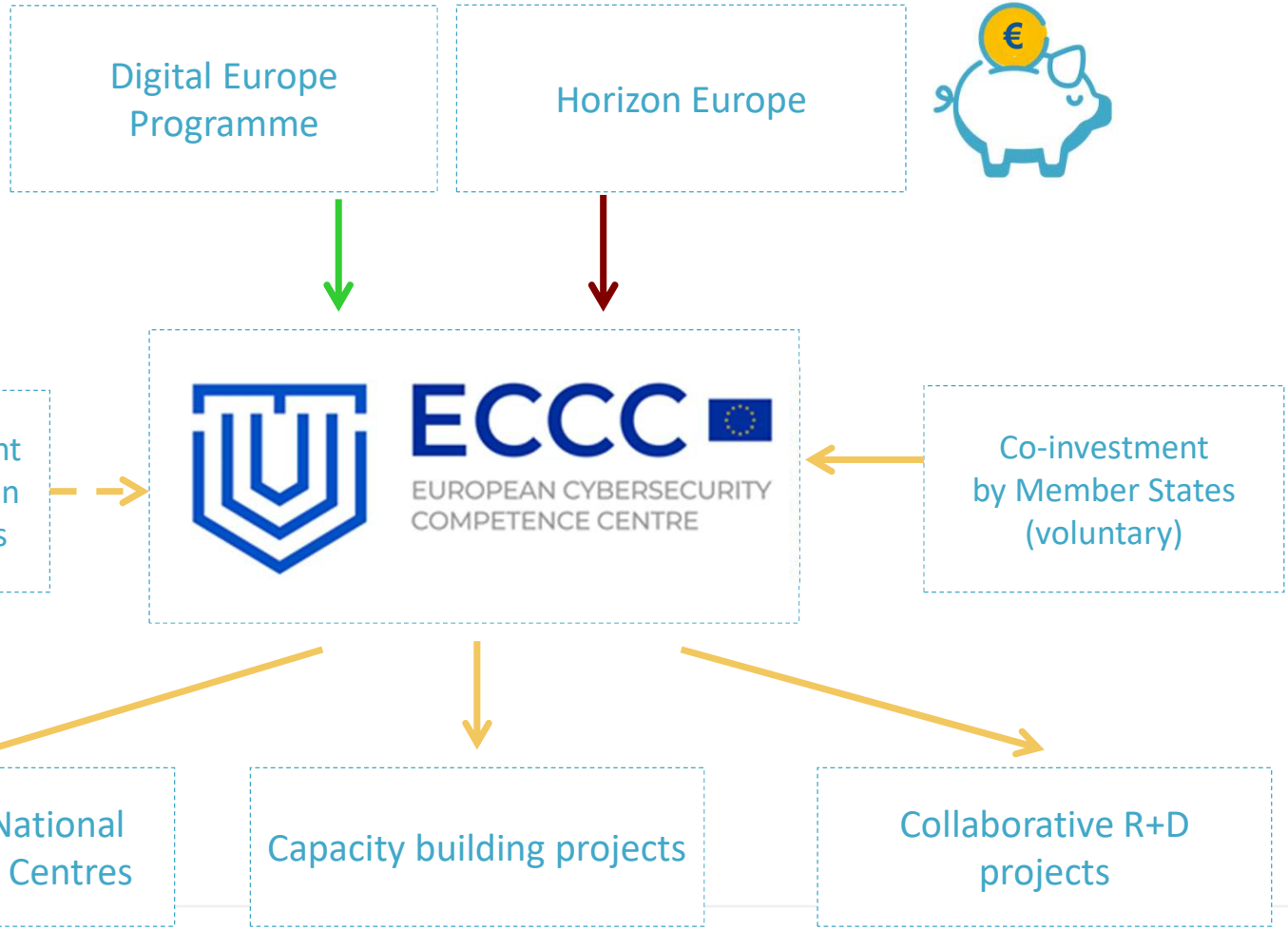
NETWORK OF NATIONAL COORDINATION CENTRES

- 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

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

2021-2027 PROPOSED EU CYBERSECURITY FUNDING SOURCES



THANK YOU FOR YOUR ATTENTION

Agamemnonos 14, Chalandri 15231
Attiki, Greece

The EU Cybersecurity Strategy for a Quantum-Safe Future

info@enisa.europa.eu

www.enisa.europa.eu