EU Cybersecurity Strategy and Capacity-building

24 June 2021

Martin Übelhör

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

THE EU'S CYBERSECURITY STRATEGY FOR THE DIGITAL DECADE

European Commission

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

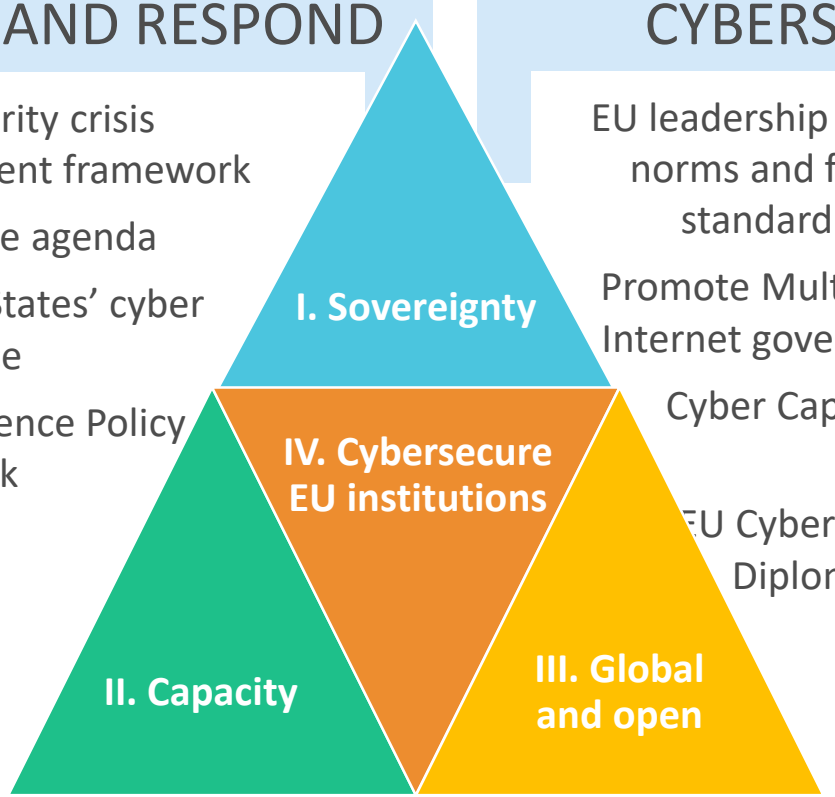
BUILDING OPERATIONAL CAPACITY TO PREVENT, DETER AND RESPOND

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

European Commission

A European Cybersecurity Technology & Innovation Ecosystem

EU Funding, Capacity-building, Community-building

European Commission

Cybersecurity knowledge and capabilities in the EU

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

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.

ECS
EUROPEAN CYBER SECURITY ORGANISATION

ECSO has +/- 250 members

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:

- 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 Commission

Stakeholders

enisa

ECS
EUROPEAN CYBER SECURITY ORGANISATION

Joint Research Centre
JRC

More than €63.5 million invested in 4 projects

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

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

Cyber Security for Europe

Partners: **43**

EU Member States involved: **20**

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

ECHO

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

SPARTA

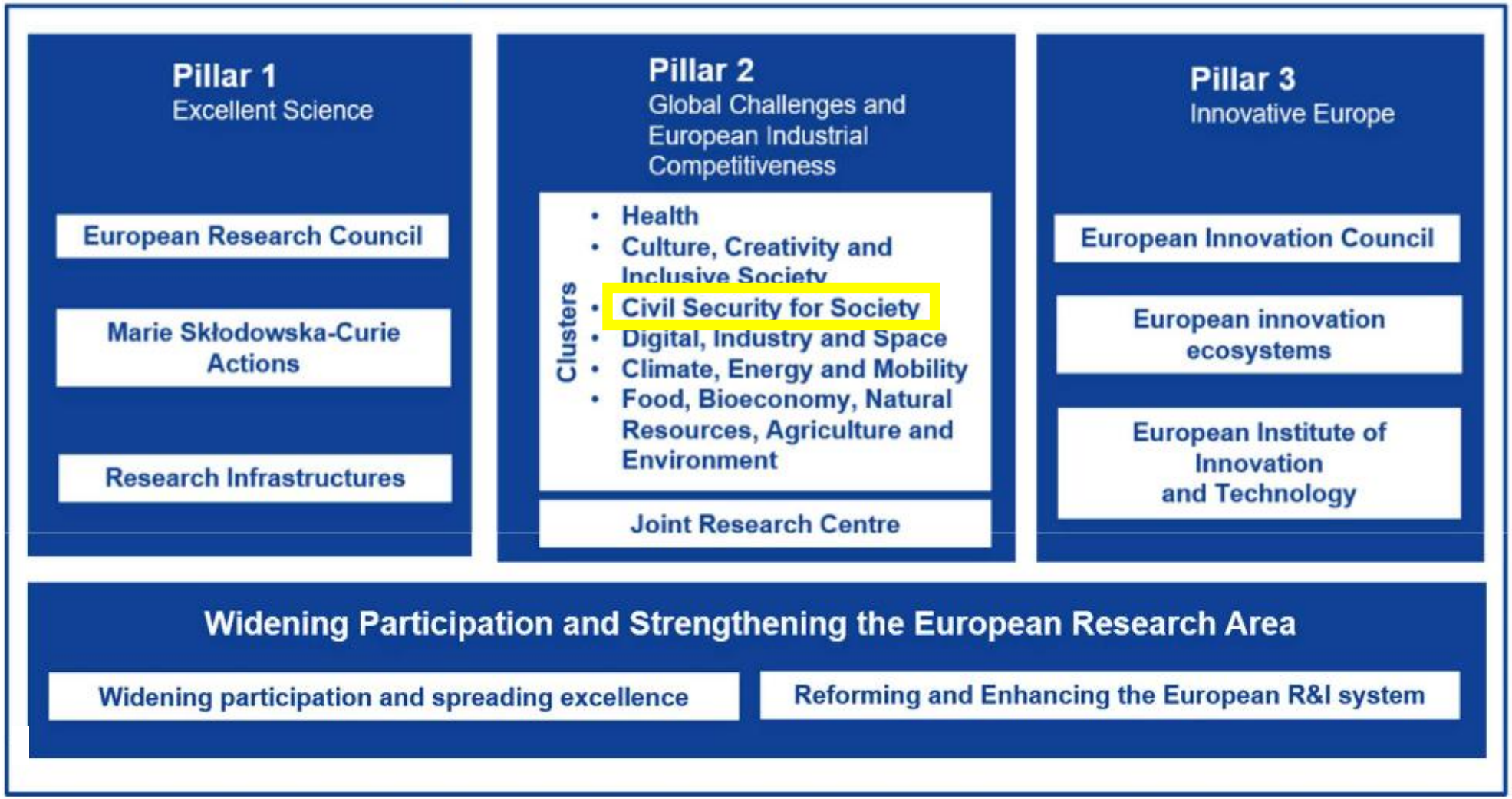
Partners: **44**

EU Member States involved: **14**

Key words
- Research Governance
- Cybersecurity skills
- Cybersecurity certification
- Community engagement
- International cooperation
- Strategic Autonomy

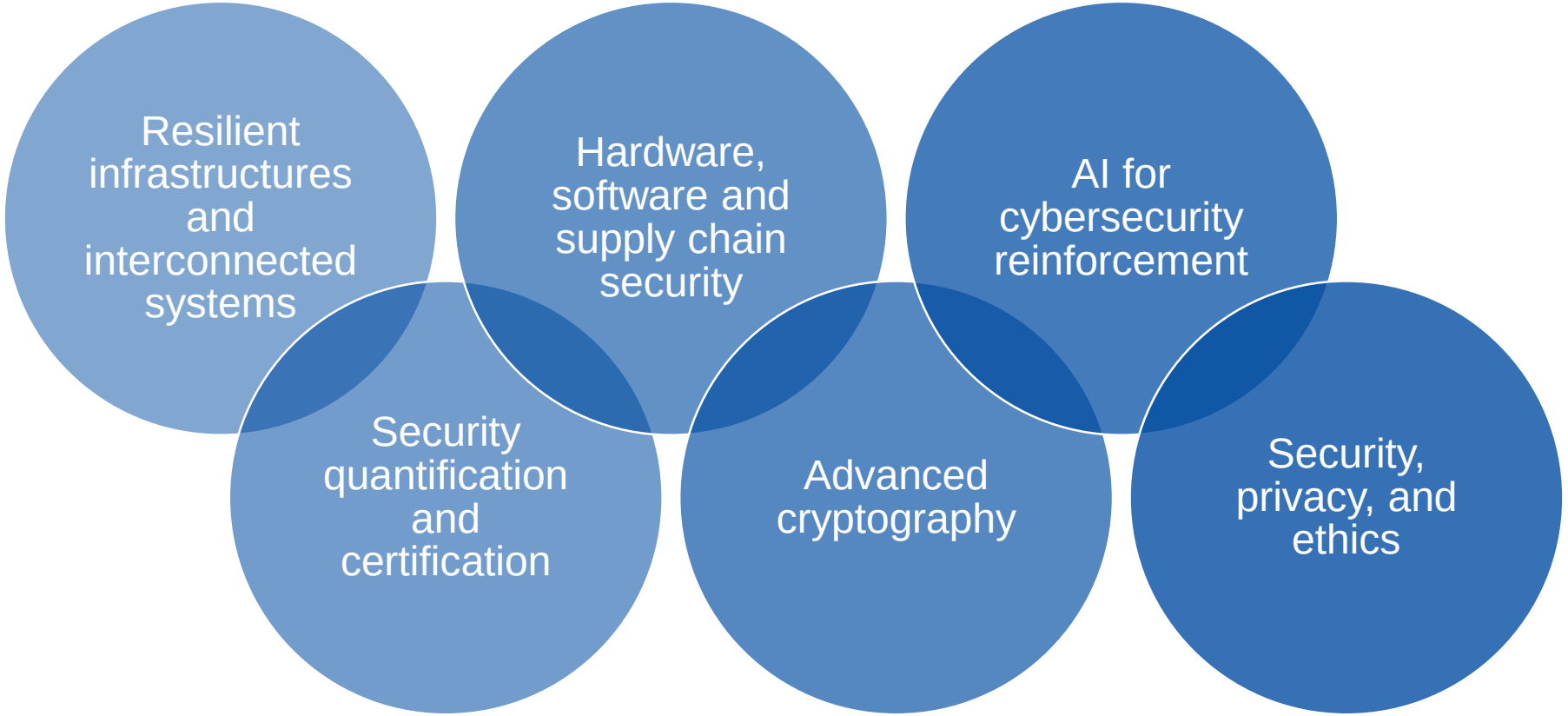
Last updated 8 March 2019

Horizon Europe - Structure



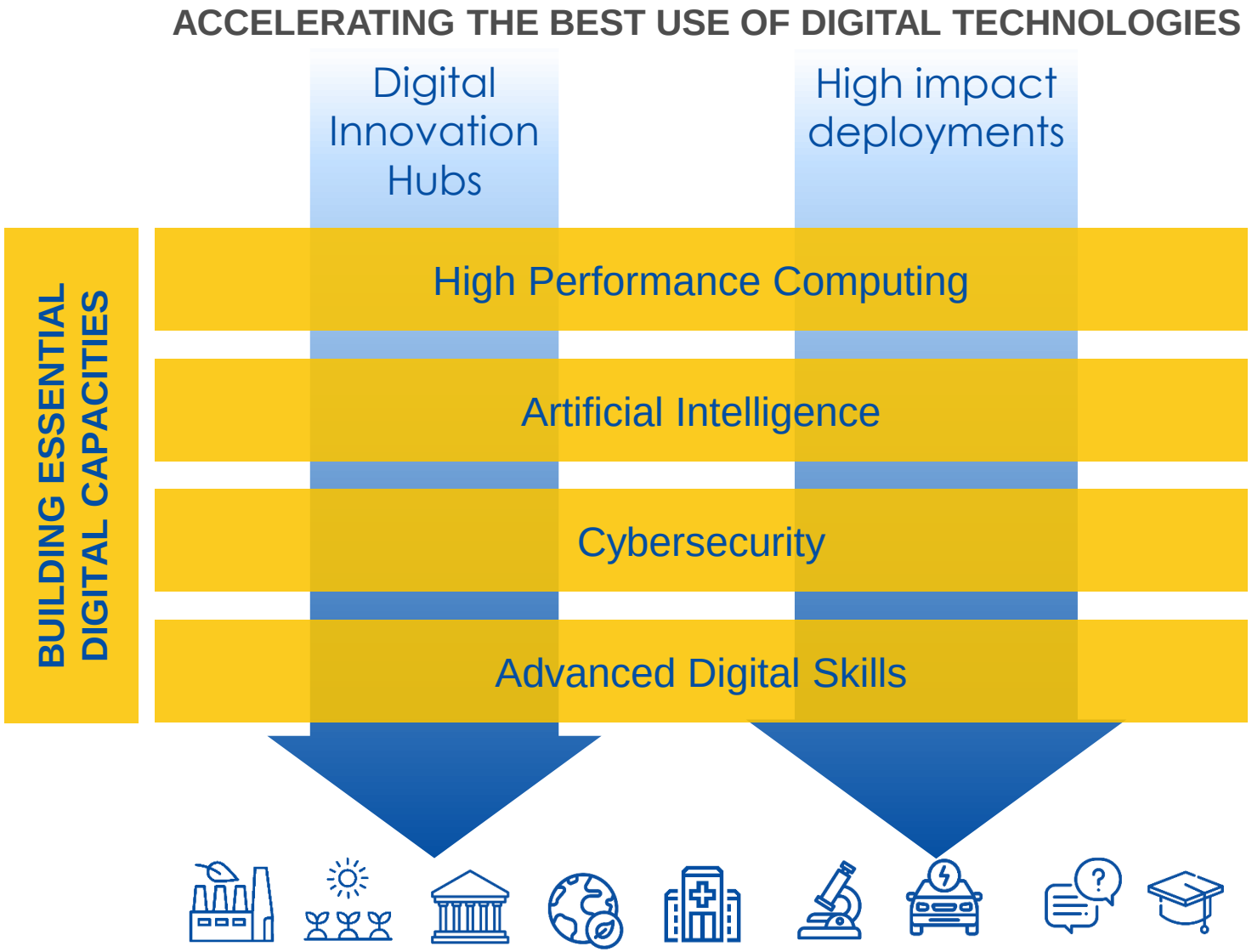
European Commission

HORIZON EUROPE (2021-2027)
Initial cybersecurity funding priorities



European Commission

Digital Europe programme structure



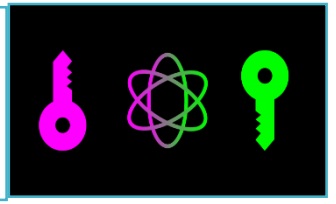
European Commission

DIGITAL EUROPE (2021 – 2027)
Initial funding priorities

Support to the network of National Coordination Centres

Key capacity building

- Quantum-secured public communication infrastructure (terrestrial segment) with the aim at deploying Quantum Key Distribution (QKD) in various large-scale networks;
- European cyber threat information network (cyber ranges);



Certification scheme(s)

- Support certification capacities
- Support SMEs to certify their products
- Provide certification testbeds;

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, …)

European Commission

Thank you

European Commission