European Cybersecurity Competence Centre and Network

EU Programmes for Cybersecurity

Swiss Innovation Briefing:

“European Cybersecurity Challenges?”

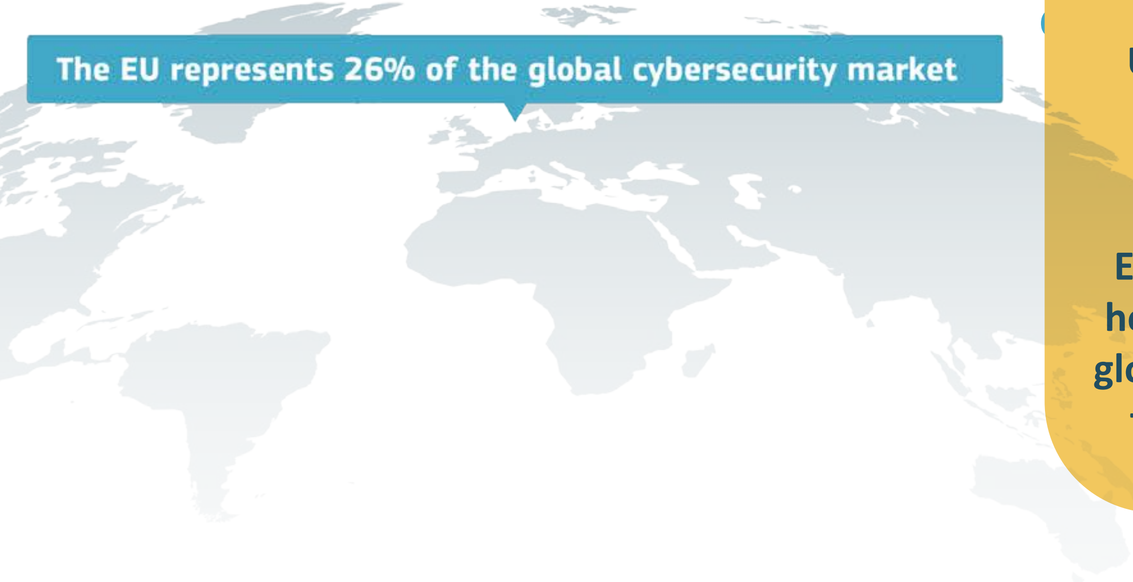
Martin Übelhör, DG CNECT

Challenges in Cybersecurity

- Capacity building, resilience
- Info sharing, joint analysis and response
- Supply chain security
- Growing attack surface (e.g. through 5G, IoT)
- Advent of AI
- Threat from quantum computing breaking “legacy” crypto

- Skills shortage
- Vulnerability of smaller organisations, SMEs
- Commercialisation of R&D
- Uptake; supply-demand articulation; single market
- Dual use
- (…)

Cybersecurity industry – where does the EU stand



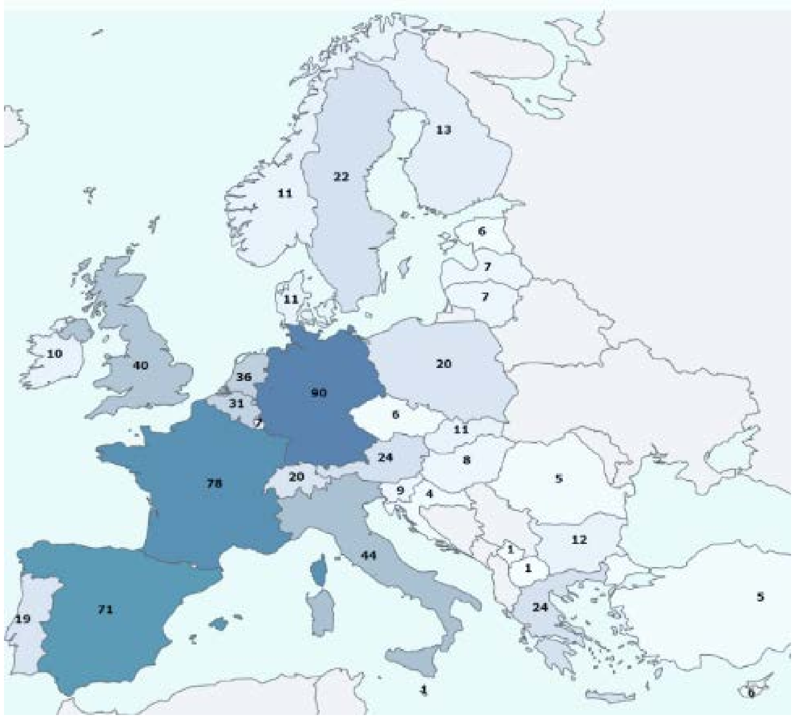
The EU represents 26% of the global cybersecurity market

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



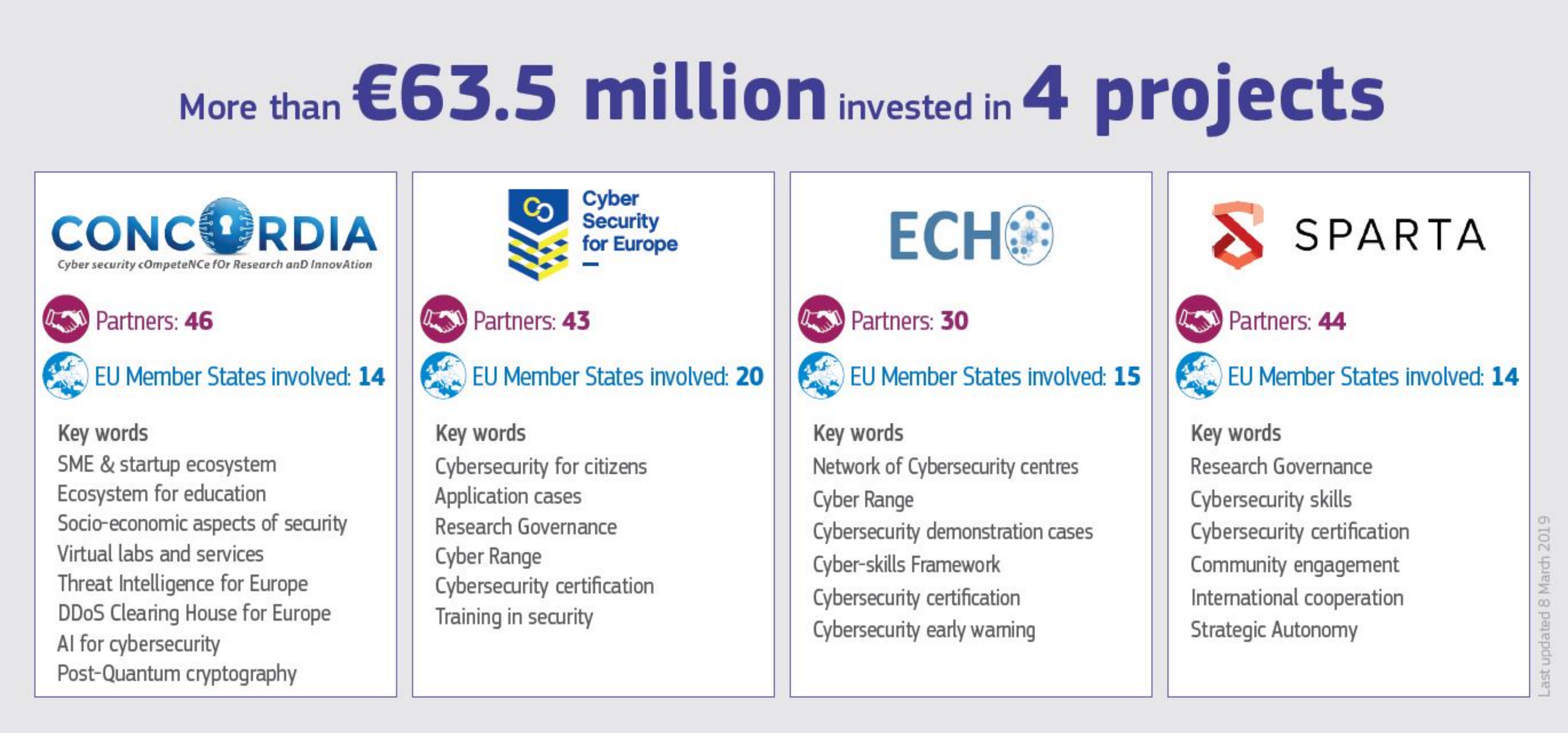
More than 660 expertise centres registered in the mapping of cybersecurity centres of expertise

ECSO has +/- 240 members

ECSO
EUROPEAN CYBER SECURITY ORGANISATION

European Commission

EU pilots helping to prepare the European Cybersecurity Competence Network



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

CONCORDIA Cyber security cOmpeteNCe fOr Research anD InnovAtion	Cyber Security for Europe	ECHO	SPARTA
Partners: **46**	Partners: **43**	Partners: **30**	Partners: **44**
EU Member States involved: **14**	EU Member States involved: **20**	EU Member States involved: **15**	EU Member States involved: **14**
Key words	Key words	Key words	Key words
SME & startup ecosystem	Cybersecurity for citizens	Network of Cybersecurity centres	Research Governance
Ecosystem for education	Application cases	Cyber Range	Cybersecurity skills
Socio-economic aspects of security	Research Governance	Cybersecurity demonstration cases	Cybersecurity certification
Virtual labs and services	Cyber Range	Cyber-skills Framework	Community engagement
Threat Intelligence for Europe	Cybersecurity certification	Cybersecurity certification	International cooperation
DDoS Clearing House for Europe	Training in security	Cybersecurity early warning	Strategic Autonomy
AI for cybersecurity			
Post-Quantum cryptography			

Last updated 8 March 2019

European Cybersecurity Technology & Innovation Ecosystem – 2018 Proposal

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

Horizon 2020 – 2020 topics (evaluations ongoing)

SU-DS02-202a0: 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)**

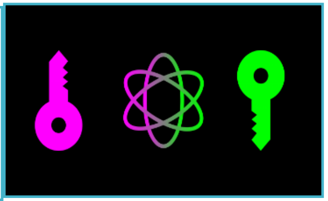
SU-AI-2020: Artificial Intelligence and security: providing a balanced assessment of opportunities and challenges for Law Enforcement in Europe **(IA, CSA 20.00 MEUR 27/08/2020)**

DIGITAL EUROPE (2021 – 2027 MFF)
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;

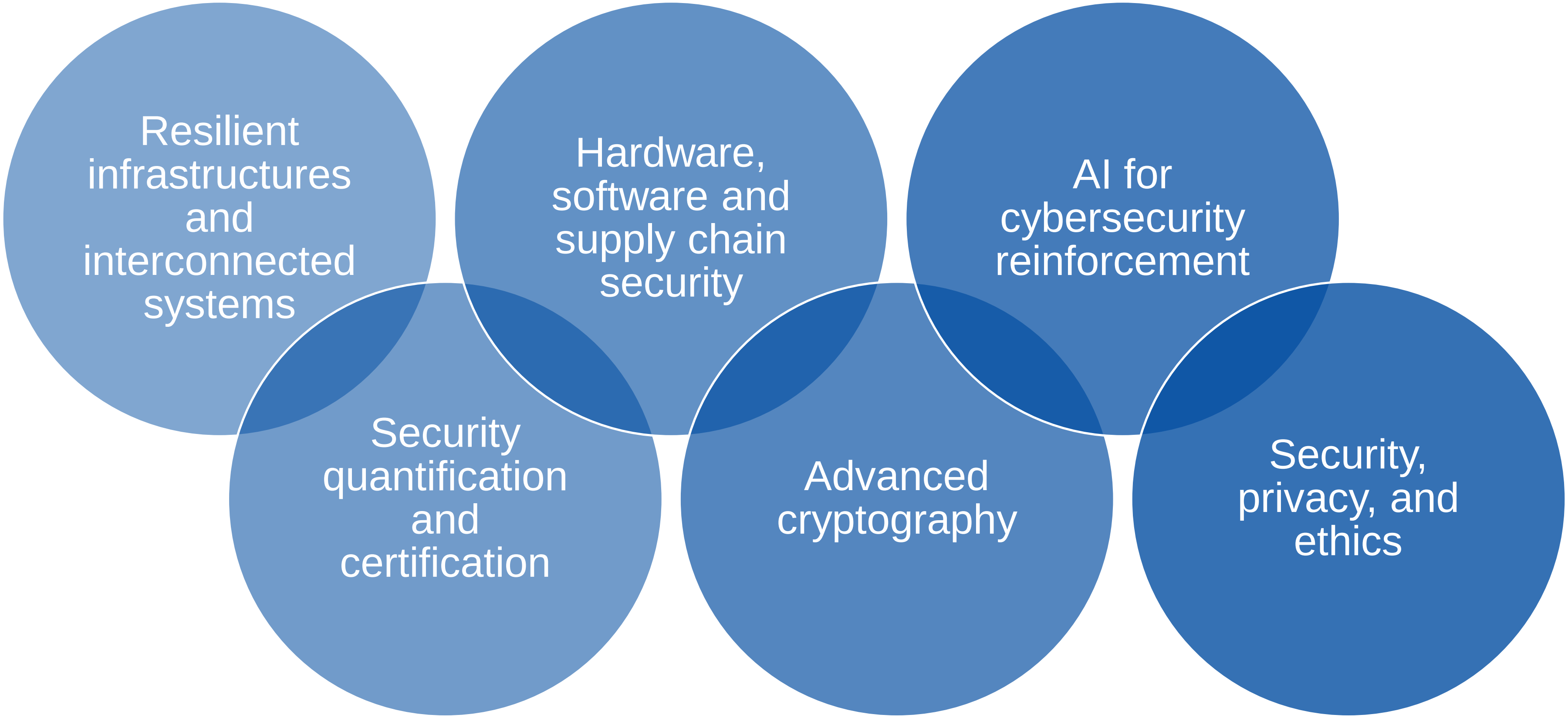
Widening the deployment of cybersecurity tools

- 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, …)

HORIZON EUROPE (2021 – 2027 MFF)
Initial cybersecurity funding priorities



Resilient infrastructures and interconnected systems

Hardware, software and supply chain security

AI for cybersecurity reinforcement

Security quantification and certification

Advanced cryptography

Security, privacy, and ethics