Cyber Security for Europe

CyberSec4Europe

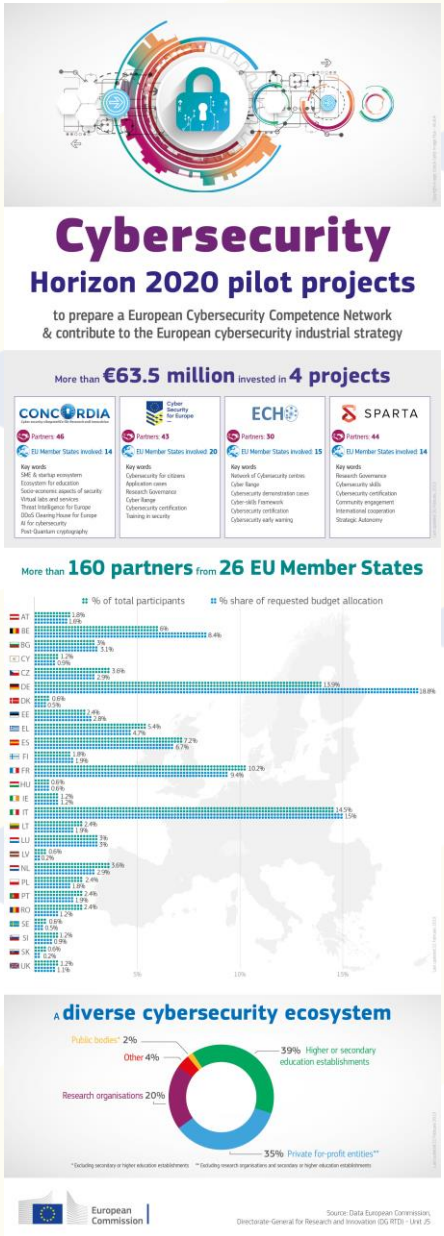
Vasileios Gkioulos, Ph.D.
Norwegian University of Science & Technology
Department of Information Security and Communication Technology
Center for Cyber and Information Security (CCIS)
Critical Infrastructure Security and Resilience group

2nd CYBERWISER workshop

CyberSec4Europe is funded by the European Union under the H2020 Programme

Grant Agreement No. 830929

Working Together Towards A Common Objective



ECHO

CONCORDIA

SPARTA

Cyber Competence Network

Cyber Security for Europe

A European network of cybersecurity centres of excellence

Changing Europe' cybersecurity research and innovation landscape

Cyber Security for Europe

Diversity and ethics

Risk acceptance

Horizontal leverage

Open leadership

NETWORK OF COMPETENCE CENTRES

Strong performers
Insufficient critical mass

Intensified partnerships
World-leading capacities

Who Are CyberSec4Europe?

43 partners in 22 countries

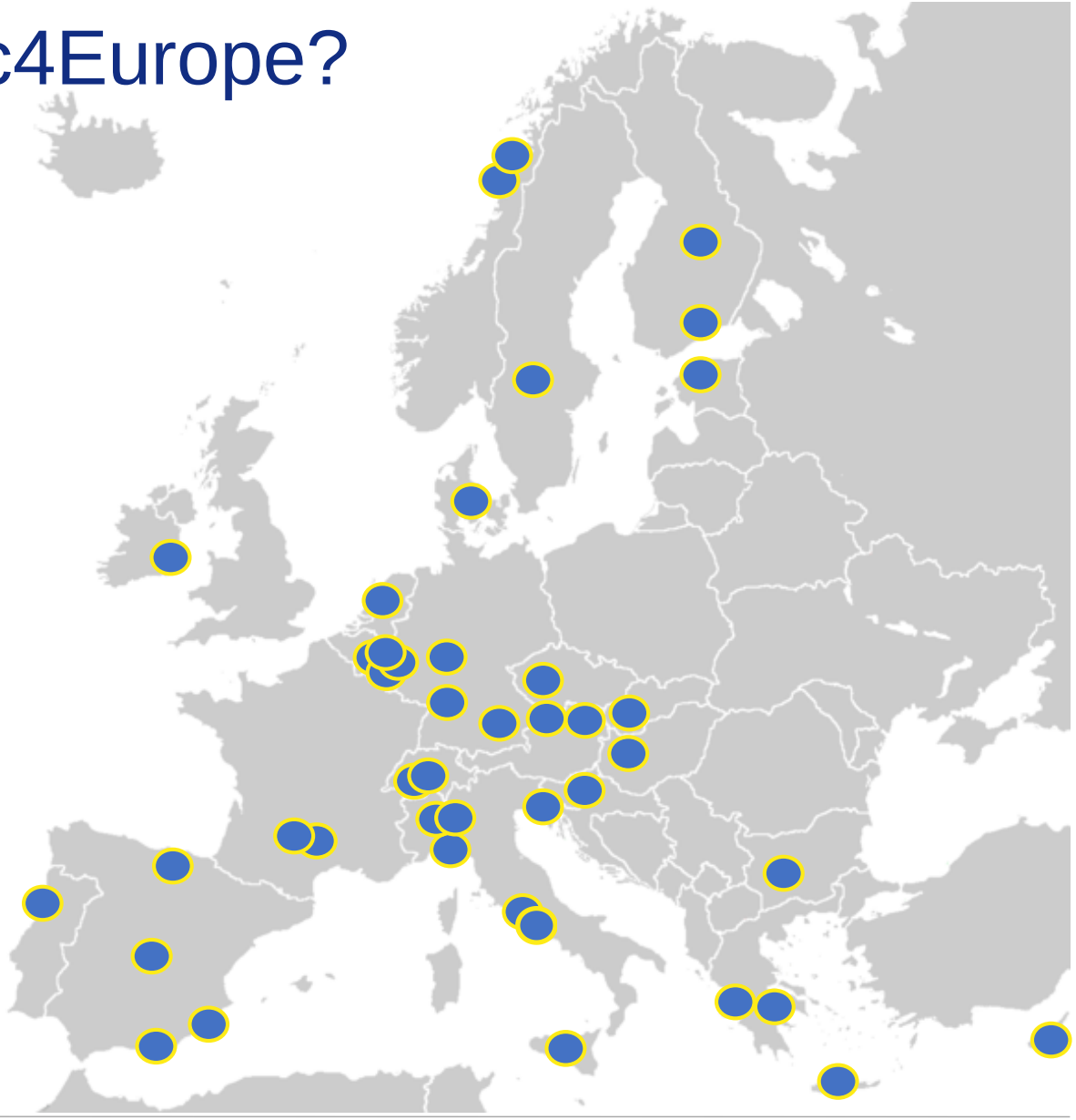
Centres of Excellence / Universities / Research Centres / SMEs

26 ECSO members involved in 6 ECSO Working Groups

Experience from over 100 cybersecurity projects in 14 key cyber domains

11 technology/ application elements and coverage of nine vertical sectors

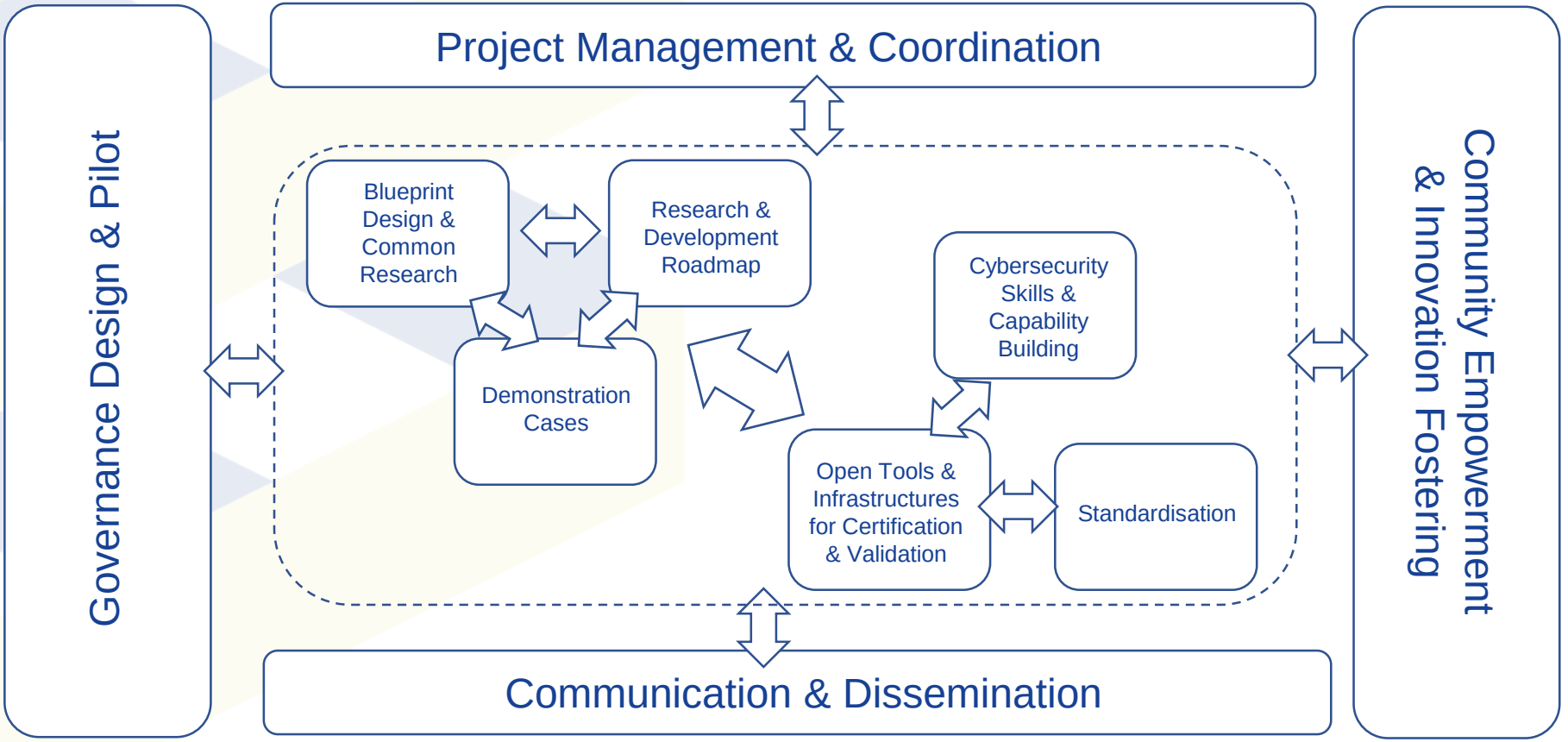
Funding period: 02/2019 – 07/2022



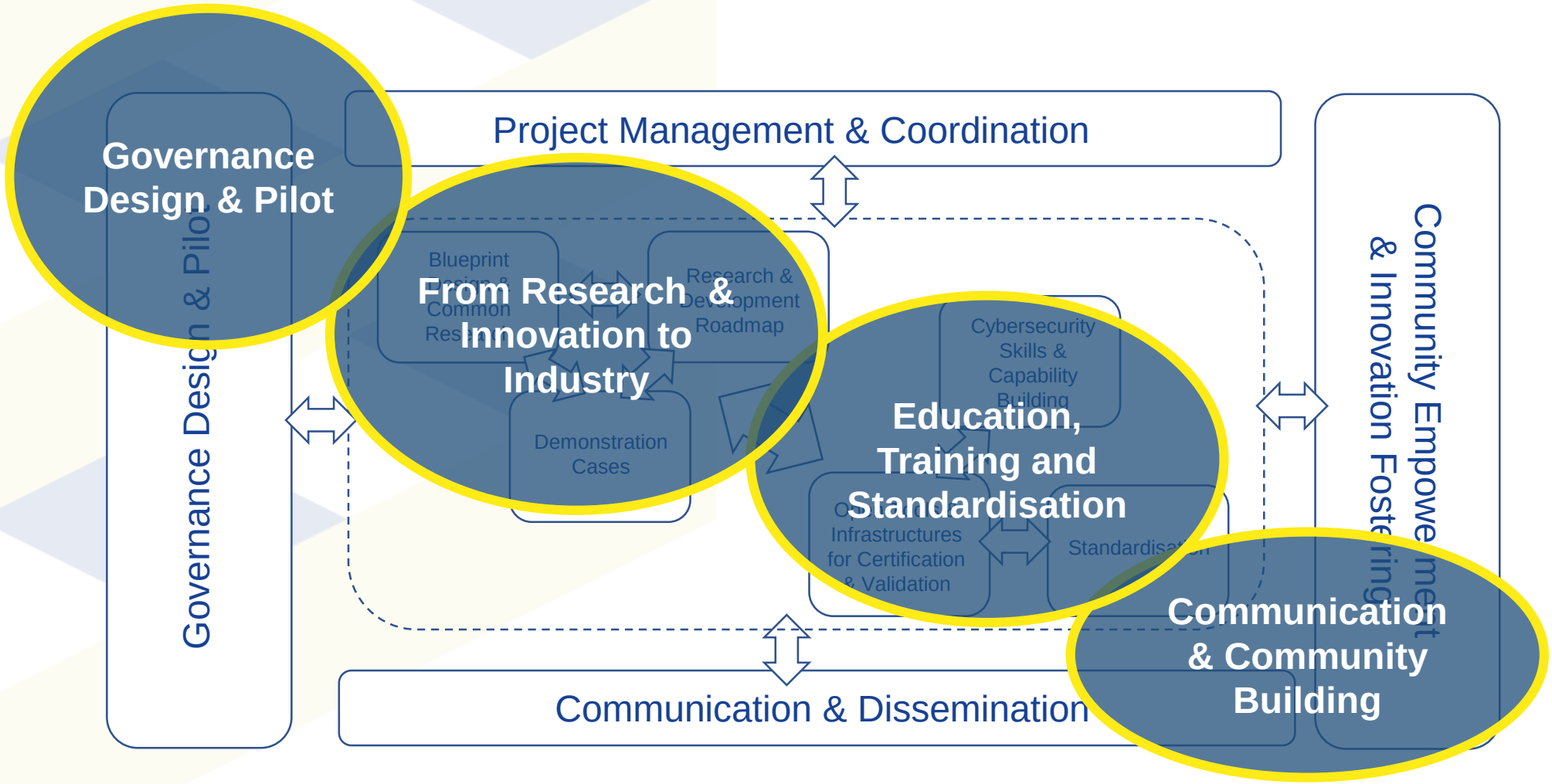
Who Are CyberSec4Europe?

Cybersecurity Expertise	KAU	UMU	AIT	FORTH	JAMK	POLITO	UCY	UMA	UNITN	UPRC	DTU	UM	NEC	CTI	SINTEF	KUL	UNILU	TUD	NTNU	CYB	ATOS	IBM	TDL	UPS-IRIT
Assurance, Audit, and Certification		X			X							X			X				X		X			X
Cryptology			X				X				X		X	X				X	X	X	X	X	X	
Data Security and Privacy	X	X	X	X	X		X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X
Education and Training	X	X	X	X	X	X	X	X	X	X	X	X		X		X		X	X				X	X
Operational Incident Handling and Digital Forensics					X			X				X						X	X		X			X
Human Aspects	X								X							X		X	X					X
Identity and Access Management (IAM)	X	X	X	X	X	X	X	X	X	X		X		X	X	X		X	X	X	X	X	X	X
Security Management and Governance	X	X	X		X				X	X		X		X	X	X		X	X	X	X	X	X	X
Network and Distributed Systems		X	X	X	X	X	X	X	X	X	X		X	X		X	X	X	X		X	X	X	X
Software and Hardware Security Engineering			X	X	X	X	X	X	X		X		X	X	X	X	X	X	X			X		X
Security Measurements	X	X	X		X	X			X					X		X		X	X	X	X			X
Technology and Legal Aspects	X		X	X		X	X	X				X		X				X	X		X		X	X
Theoretical Foundations of Security Analysis and Design			X			X		X			X			X			X	X	X	X		X		X
Trust Management, Assurance, and Accountability		X			X	X		X		X	X			X	X	X					X		X	X

Piloting a Competence Network



Piloting a Competence Network



Demonstration Cases by Industrial Sectors

Cyber Security for Europe

Finance

- Incident reporting
- PSD2 / GDPR issues

Health

- Medical data exchange

Smart Cities

- Citizen participation/e-Government
- Critical infrastructures
- Education

Transport

- Maritime (port critical infrastructure)
- Supply chain assurance

Boost the success of businesses and protect the rights of citizens in the EU.

- Common Framework Design
- Research and Integration on Cybersecurity Enablers and underlying Technologies
- Software Development Lifecycle
- Security Intelligence
- Adaptive Security
- Usable security
- Regulatory sources for citizen-friendly goals
- Conformity, Validation, and Certification
- Continuous Scouting
- Impact on Society

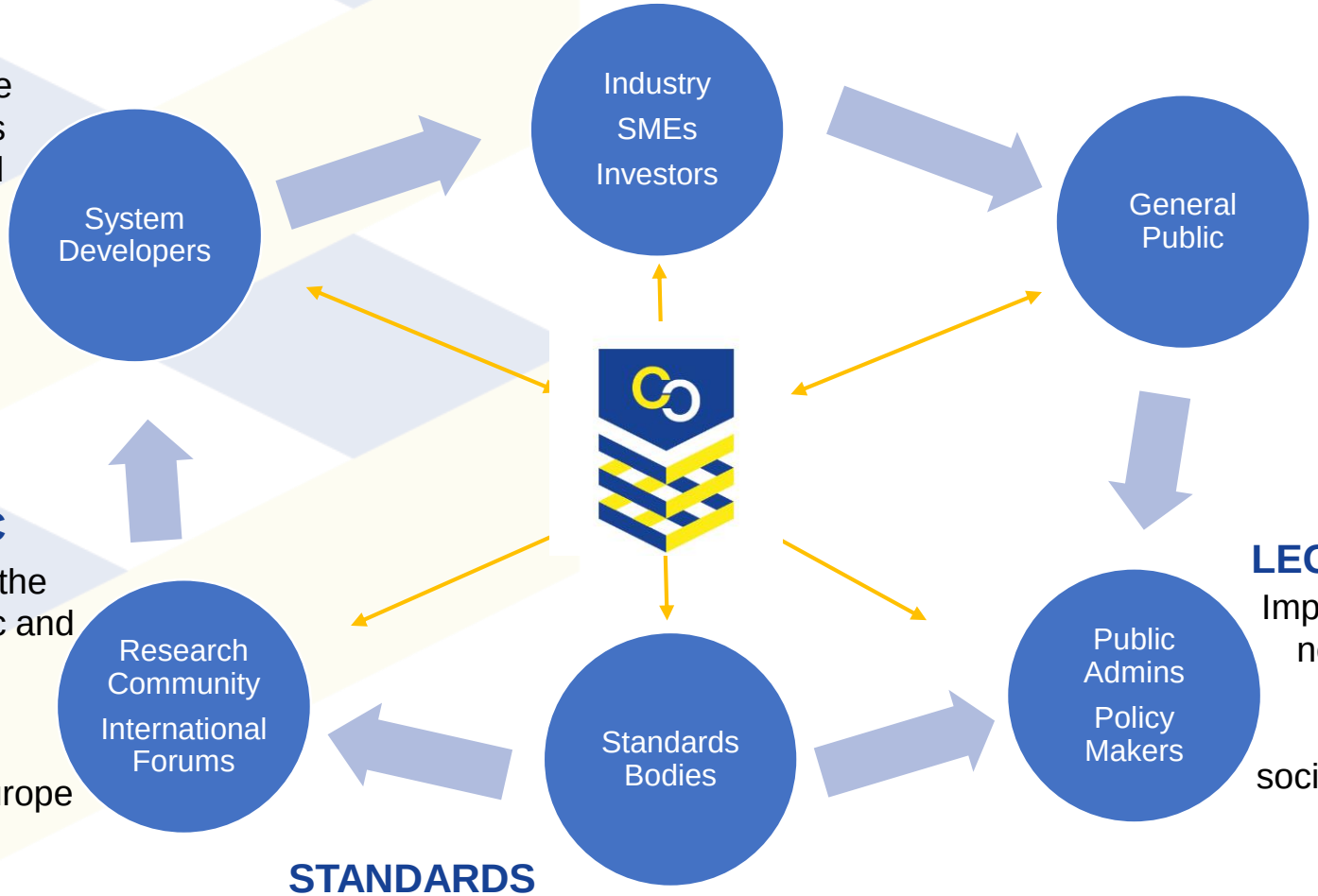
- Task 3.10: Impact on Society
  - This task will be devoted to analyse and identify efficient measures and methods for the continuous enhancement of societal security awareness, which should be held regularly to ensure that the staff is knowledgeable regarding the up-to-date security solutions, referring to private usage of digital technologies, human aspects of information security, professional practice and competence-development, governance, management and achievement of results
- Task 9.4: Raising security awareness
  - This task will be devoted to analyse and identify efficient measures and methods for the continuous enhancement of societal security awareness, to ensure that the staff is knowledgeable regarding the up-to-date security solutions, referring to private usage of digital technologies, human aspects of information security, professional practice and competence-development, governance, management and achievement of results. One essential target group is SMEs with focus on the potentially serious cybersecurity problems that these SMEs may face and generate for a whole supply chain.

Cybersecurity Stakeholders

Cyber Security for Europe

BUSINESS Business opportunities and potential of technology and societal benefits

TECHNICAL
Understandable by ICT systems developers and system managers



SOCIAL
Understandable by a large public of non-specialists

SCIENTIFIC
High level on the main scientific and technical innovation addressed by CyberSec4Europe

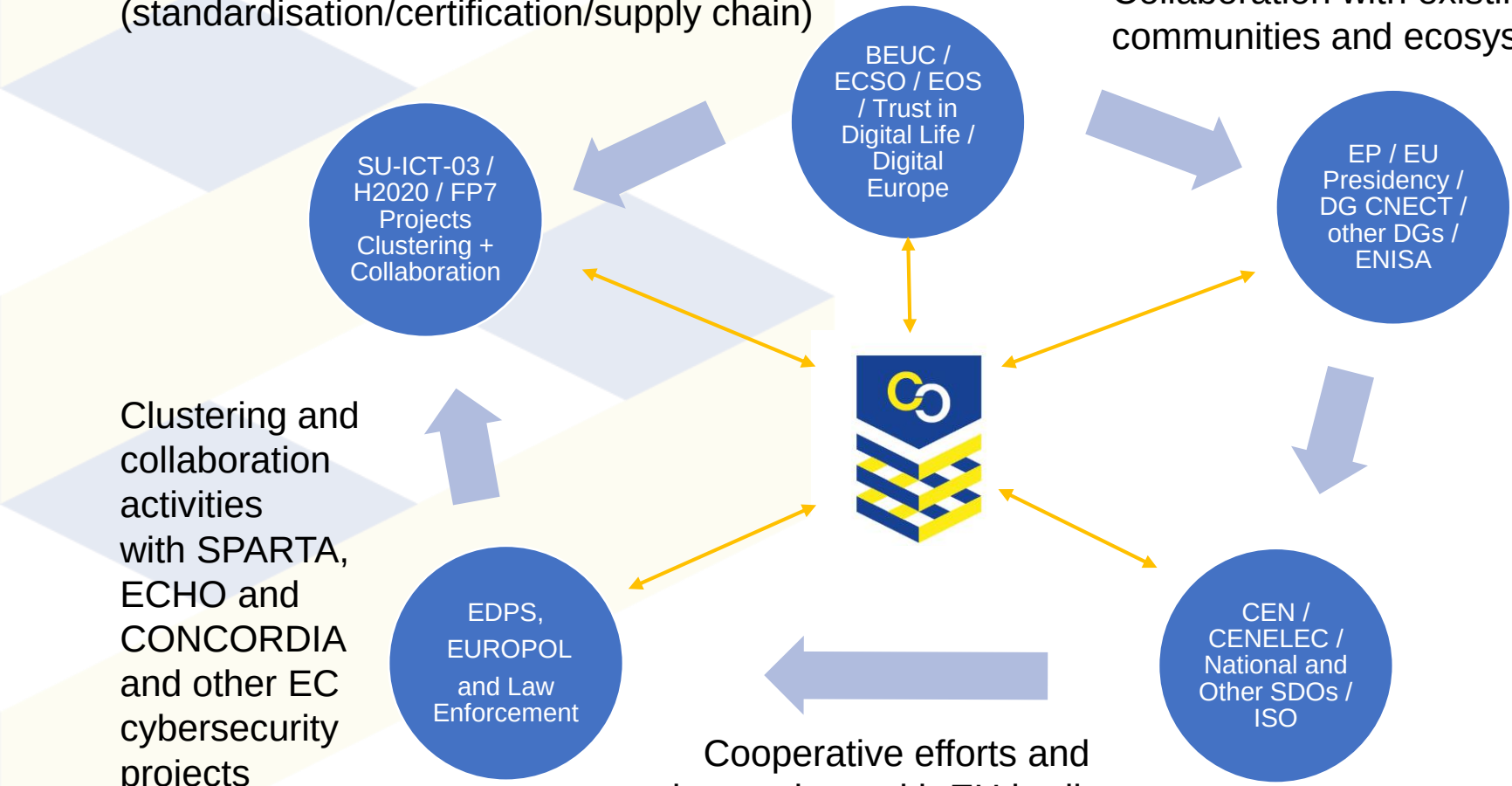
LEGISLATIVE
Implementation of new EU privacy and security regulation and social implications

STANDARDS

Community Empowerment and Innovation Fostering

Close working relationship with ECSO WG1 (standardisation/certification/supply chain)

Collaboration with existing cybersecurity communities and ecosystems innovation



Clustering and collaboration activities with SPARTA, ECHO and CONCORDIA and other EC cybersecurity projects

Cooperative efforts and interactions with EU bodies

Cyber Security for Europe

Thank you

Vasileios Gkioulos, Ph.D.
Norwegian University of Science & Technology
Department of Information Security and Communication Technology
Center for Cyber and Information Security (CCIS)
Critical Infrastructure Security and Resilience group