Cyber
Security
for Europe

CyberSec4Europe

Kai Rannenberg, Goethe University Frankfurt

SEREN4 Workshop
2020-04-28
Vienna, virtual

CyberSec4Europe is funded by the European Union under the H2020 Programme

Grant Agreement No. 830929

Who Are CyberSec4Europe?

Centres of Excellence / Universities / Research Centres / SMEs

43 partners in 22 countries

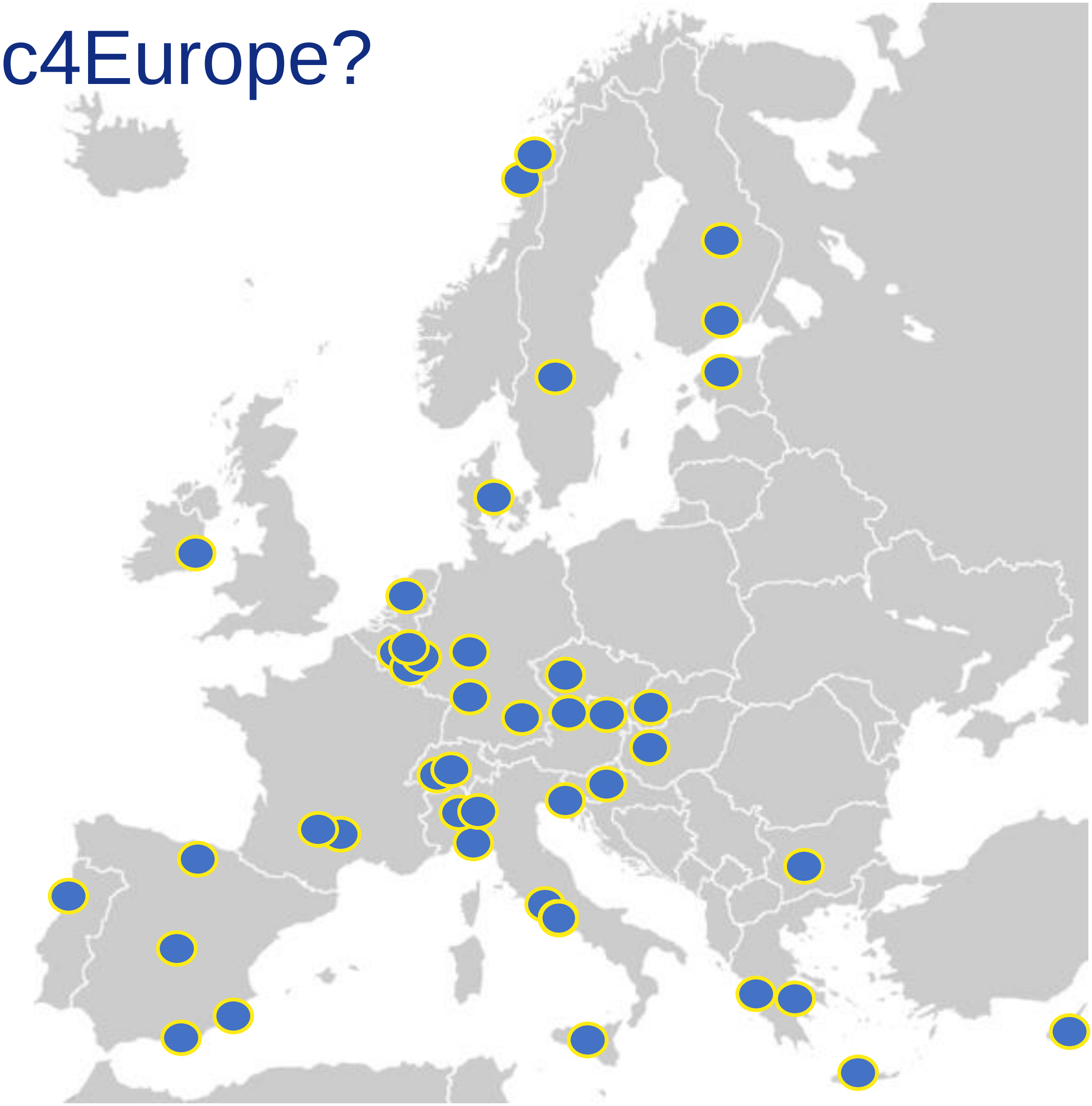
11 technology/application elements and coverage of nine vertical sectors

Experience from over 100 cybersecurity projects in 14 key cyber domains

26 ECSO members involved in 6 ECSO Working Groups

Existing networks (ECSO, TDL, EOS, CEPIS)

Funding period:
02/2019 – 07/2022



Consortium Partners: Universities & Knowledge Institutes

Germany

Goethe University Frankfurt

The Netherlands

TU Delft

Spain

University of Malaga

University of Murcia

Portugal

University Porto

Finland

JAMK University of Applied Sciences

Sweden

Karlstad University

Cyprus

University of Cyprus

Greece

University of Piraeus

CTI “Diophantus” Patras

FORTH

Slovenia

University of Maribor

Luxembourg

University of Luxembourg

France

Université Paul Sabatier Toulouse / IRIT

Norway

NTNU

SINTEF

Italy

CNR

POLITO

Trento University

Ireland

University College Dublin (LERO)

Belgium

KU Leuven

Denmark

Denmark Technical University

Austria

AIT

Czech Republic

Masaryk University Brno

Consortium Partners: Industry, SMEs and Others

Industrial

Italy:	ABI Lab Engineering Spa Intesa Sanpaolo
Germany:	NEC Labs Europe
	Siemens AG
France:	Banque Populaire
	DAWEX
Spain:	Banco Bilbao Argentaria
Estonia:	Cybernetica
Spain:	ATOS Spain
Finland:	VTT

SMEs

Switzerland:	Conceptivity
	Archimede Solutions
Bulgaria:	International Cyber Investigation Training Academy
Belgium:	Open & Agile Smart Cities
	Time.Lex
Slovakia:	VaF

Local Government

Italy:	Comune di Genova

Association

Belgium:	Trust in Digital Life

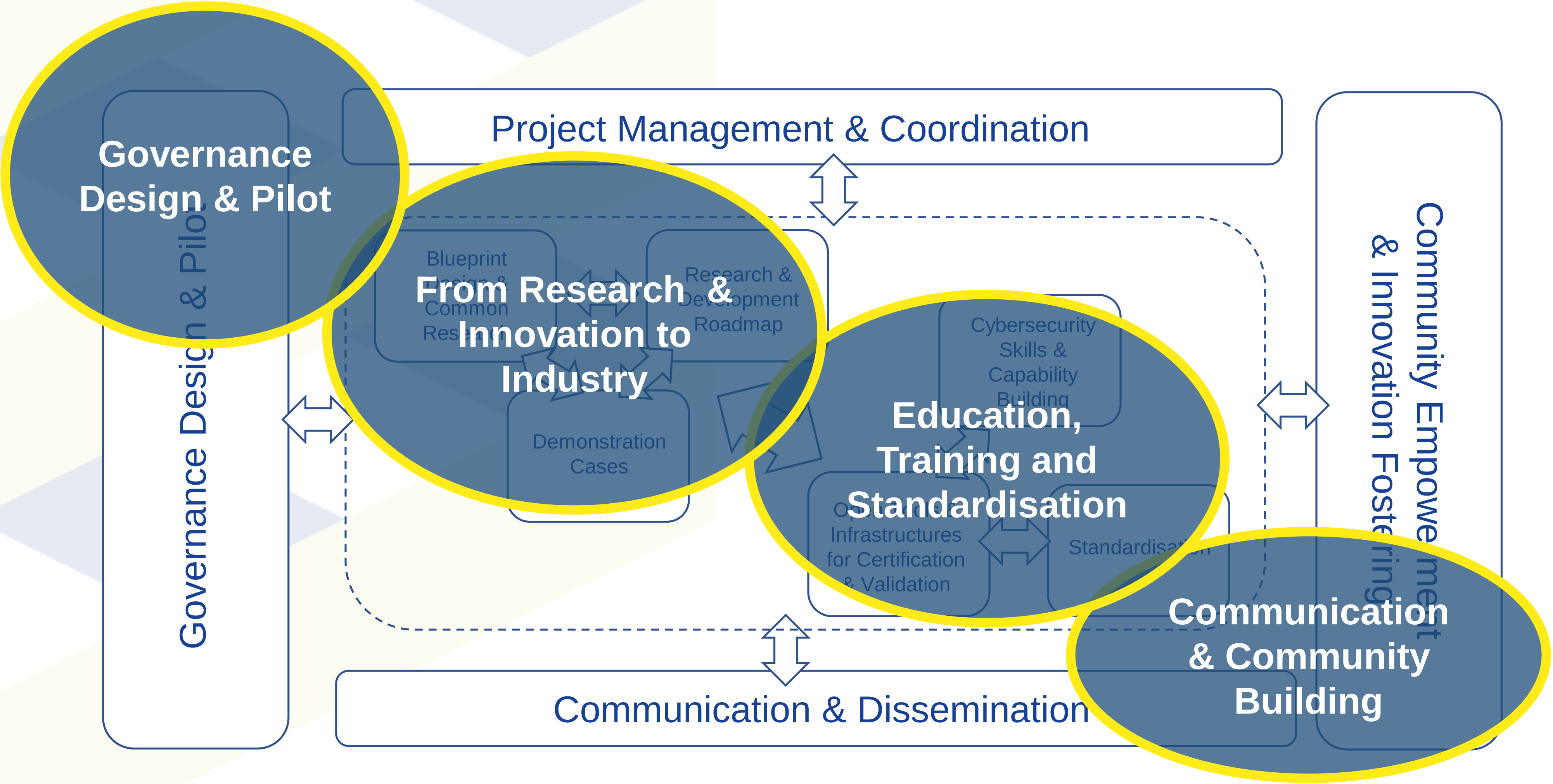
About CyberSec4Europe

Cyber Security for Europe

CyberSec4Europe is a research-based consortium working across four different but inter-related areas with a strong focus on openness and citizen-centricity in order to:

- Pilot a European Cybersecurity Competence Network
- Design, test and demonstrate potential governance structures for the network of competence centres
- Harmonise the journey from software componentry identified by a set of roadmaps leading to recommendations
- Ensure the adequacy and availability of cybersecurity education and training as well as common open standards
- Communicate widely and build communities

Piloting a Competence Network



Governance Design & Pilot

From Research & Innovation to Industry

Education, Training and Standardisation

Communication & Community Building

Project Management & Coordination

Governance Design & Pilot

Blueprint Design & Common Research

Research & Development Roadmap

Demonstration Cases

Cybersecurity Skills & Capability Building

Operational Infrastructures for Certification & Validation

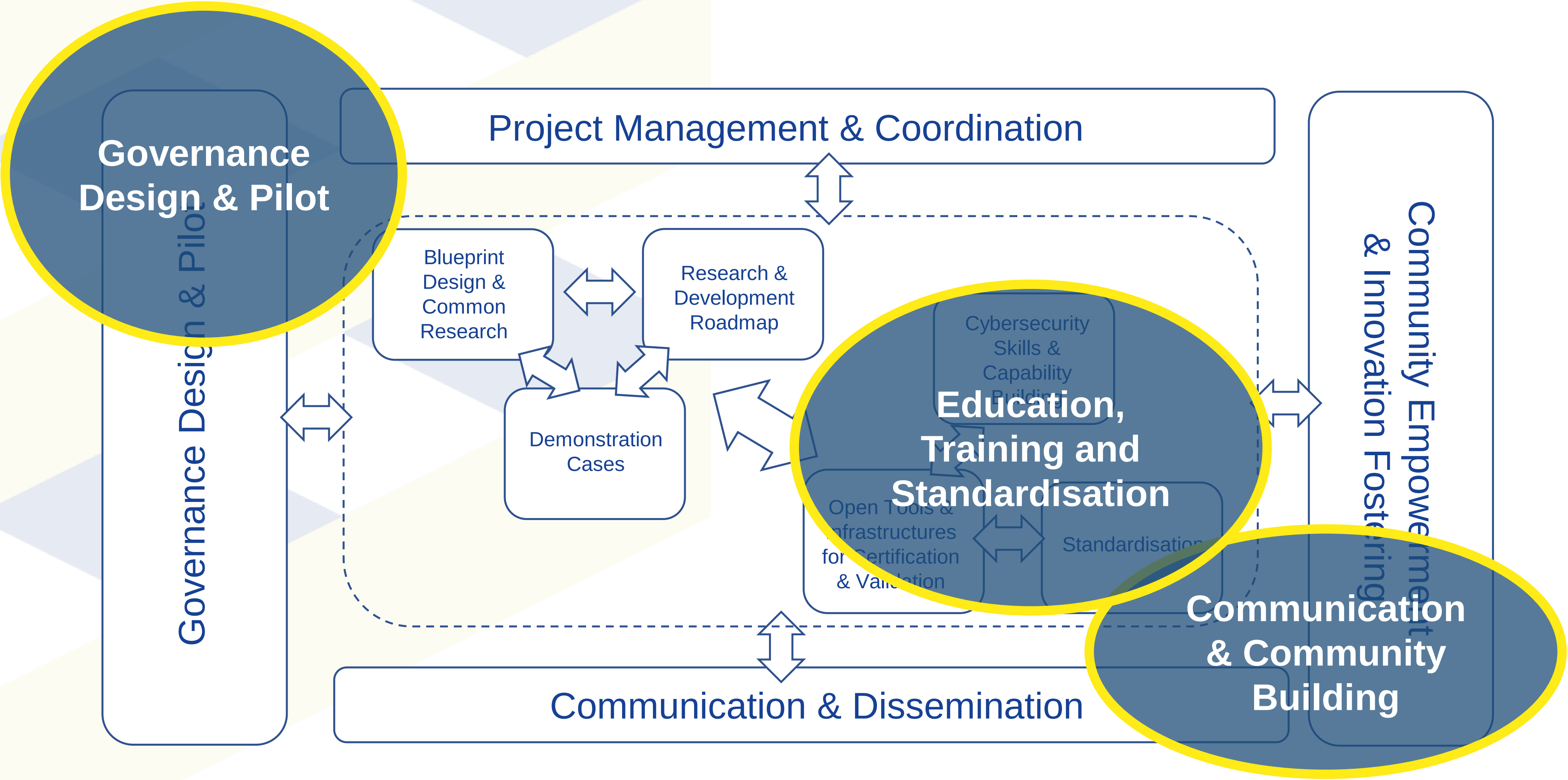
Standardisation

Community Empowerment & Innovation Fostering

Communication & Dissemination

Cyber Security for Europe

From Research & Innovation to Industry



Governance Design & Pilot

Project Management & Coordination

Governance Design & Pilot

Blueprint Design & Common Research

Research & Development Roadmap

Demonstration Cases

Cybersecurity Skills & Capability Building

Education, Training and Standardisation

Open Tools & Infrastructures for Certification & Validation

Standardisation

Community Empowerment & Innovation Fostering

Communication & Community Building

Communication & Dissemination

From Research & Innovation to Industry

Cyber Security for Europe

Development of software assets

Short and long term sector roadmaps

Demonstration use cases

Finance

- Incident reporting
- Open Banking

Health

- Medical data exchange

Smart Cities

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

Transport

- Maritime (port critical infrastructure)
- Supply chain assurance

Copyright 2020

Matching Industry Demonstrators with Blueprint Research

Application Demonstrators

Finance

- Incident reporting
- PSD2 / GDPR issues

Health

- Medical data exchange

Smart Cities

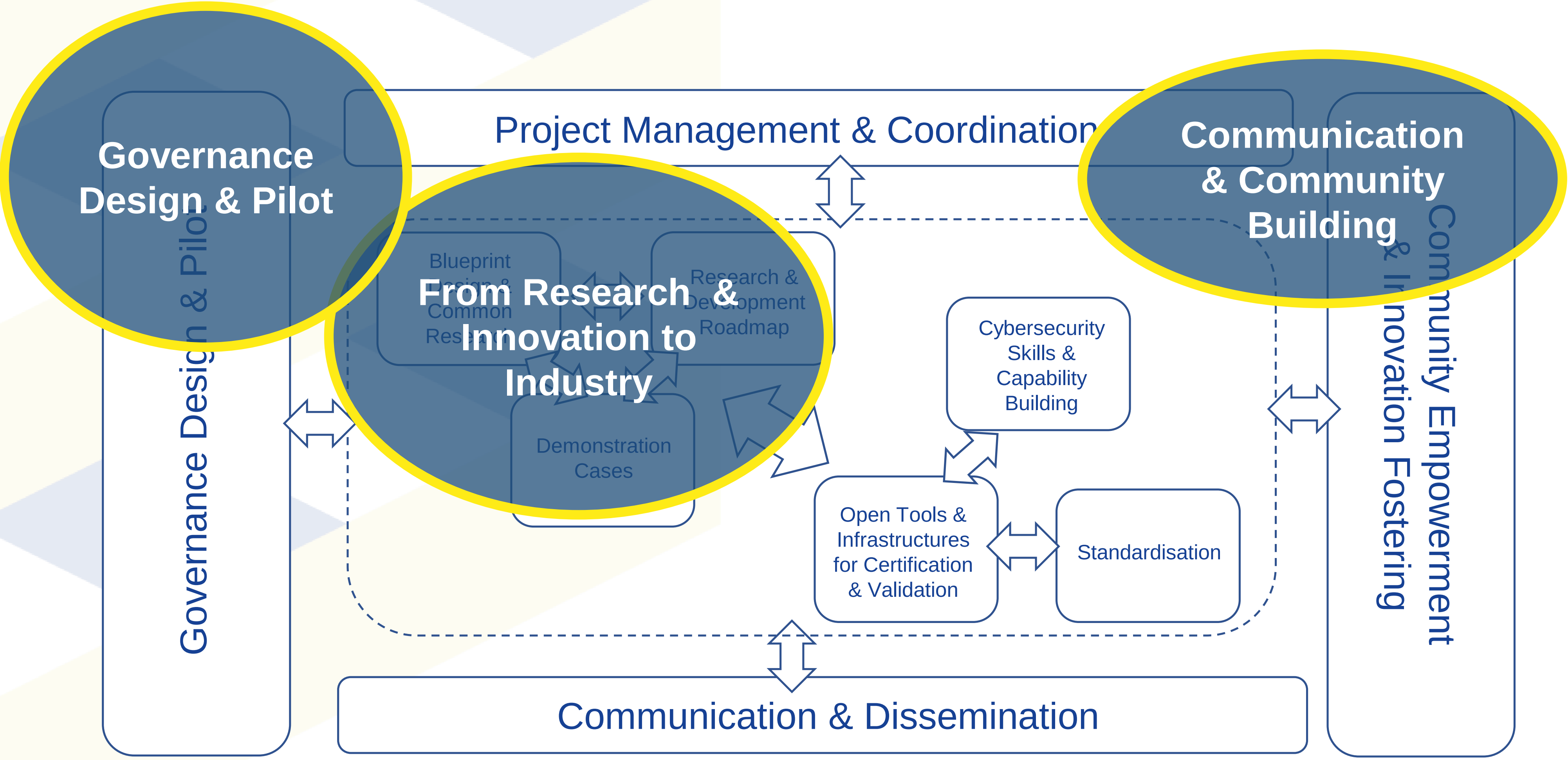
- Citizen participation/e-Government
- Critical infrastructures
- Education

- Transport
  - Maritime assurance
  - Supply chain

Blueprint Research

- Research and integration on cybersecurity enablers and underlying technologies
- SDL - software development lifecycle
- Security intelligence
- Adaptive security
- Usable security
- Regulatory sources for citizen-friendly goals
- Conformity, validation and certification
- Continuous scouting
- Impact on society

Education, Training & Standardisation


Governance Design & Pilot
From Research & Innovation to Industry
Communication & Community Building
Governance Design & Pilot
Project Management & Coordination
Blueprint Design & Common Research
Research & Development Roadmap
Demonstration Cases
Cybersecurity Skills & Capability Building
Open Tools & Infrastructures for Certification & Validation
Standardisation
Community Empowerment & Innovation Fostering
Communication & Dissemination

Cybersecurity Skills & Capability Building

- Combines formal, professional and non-traditional skill building

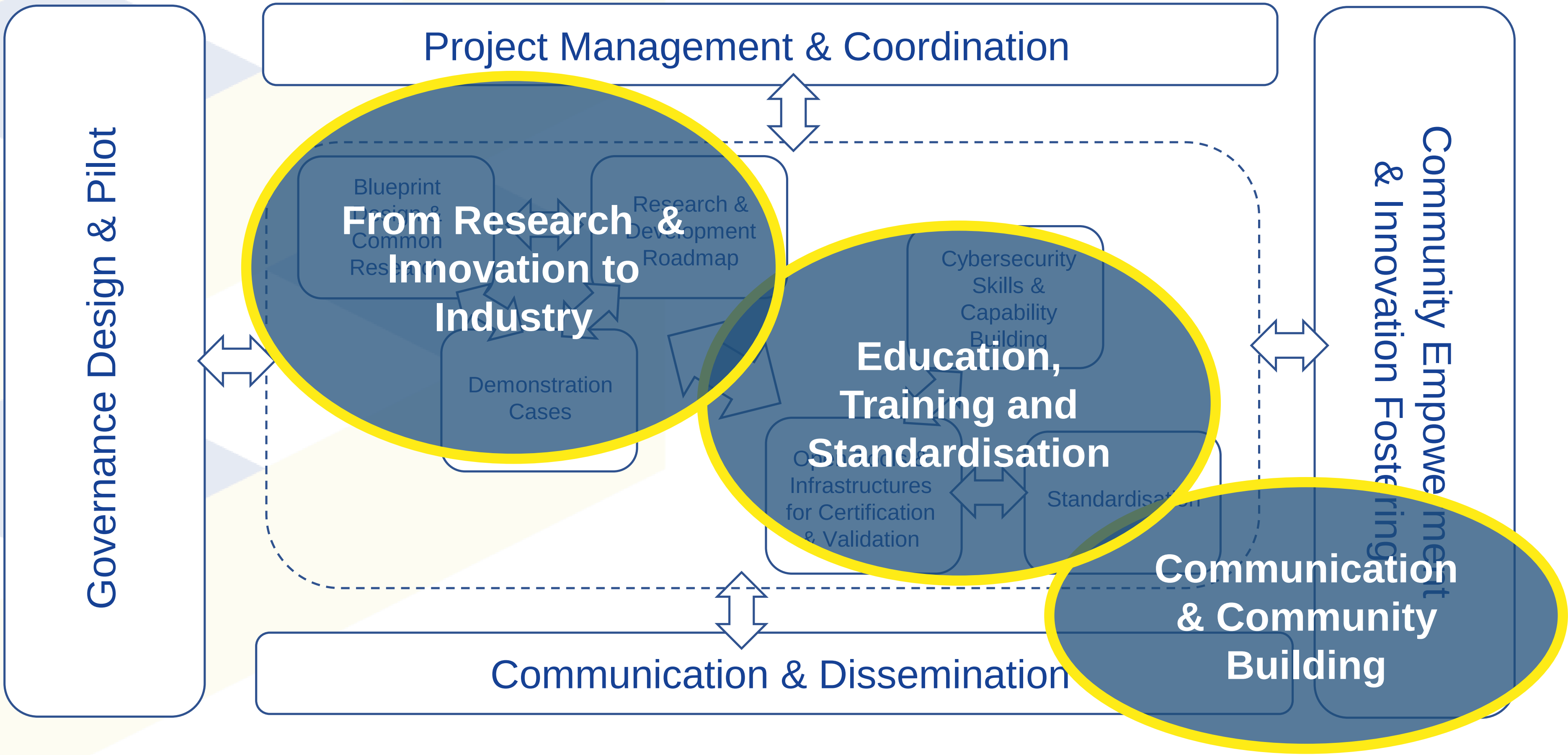
- University education → Map education in Europe
- Professional training and workforce assessment
- Virtual education
  - Quality branding of MOOC education was the first pilot of governance delivered in the summer
- Cyber ranges as platform for education, training

Standardisation

- Increase economic impact of EU R&I → disseminating EU Tech into international standards

- Maintaining contacts with standardisation organisations
- Assessing existing procedures in the context of cybersecurity
- From technical work → standards
- Bring together standards projects and key cybersecurity experts

Governance Design & Pilot


Project Management & Coordination
Governance Design & Pilot
Community Empowerment & Innovation Fostering
Blueprint Design & Common Research
Research & Development Roadmap
Demonstration Cases
Cybersecurity Skills & Capability Building
Open Common Infrastructures for Certification & Validation
Standardisation
Communication & Dissemination
From Research & Innovation to Industry
Education, Training and Standardisation
Communication & Community Building

Governance Design & Tasks

Cyber Security for Europe

- Collecting Stakeholders' viewpoints
  - If you have strong opinions → UTrento likes to interview you
- Assessing best governance practices
  - Top-down vs. bottom up
  - Civil society (academia, NGOs, industry) involvement vs. government/admin (police, SIGINT, military) involvement
- Governance structure
  - Design: enable bottom-up advice
  - Operation and testing: MOOCs and regional hub in Toulouse
- Preparation for the implementation
  - Regional vs. national
    - Pilot regional competence hub in Toulouse
    - National hub candidate in Denmark

Examples of competence centres “in” CyberSec4Europe

- Nationwide hubs
  - Topically open and rather general
  - Danish Hub for Cybersecurity (Denmark)
- Regional Community hubs of expertise
  - Topically open and rather general
  - OcSSImore/CHECK (Toulouse, France)
- Topically focussed hubs
  - Rather nationwide than regional
  - JYVSECTEC National Cyber Range Ecosystem (Finland)
  - CyberChallenge.IT for young cyber talent (Italy)

Lessons learned and being learned Collected and distilled by WP2

- The **low** level of **collaboration** between **academia** and **industry** in the EU is a systemic problem that is visible in the leading cybersecurity research venues where innovative work is published.
  - No definitive explanation for this pattern, suggest a lack of resources for research and development.
  - Broken chain between purely academic → applied work (both at research and education)

➢ New **governance structure** can**not** just be a **platform** → **address lack** of **investment**, if Europe wants to better capitalize on the synergies from joint R&D by academia and industry.

  ➢ EC as coordinating role

  ➢ MS and local stakeholders as setting priorities (depending on local strength and opportunities)

➢ **Synergy** between **top-down** and **bottom-up** structures → **integrating stakeholder** groups, → leading to efficient stakeholder **engagement** throughout **all societal levels**.

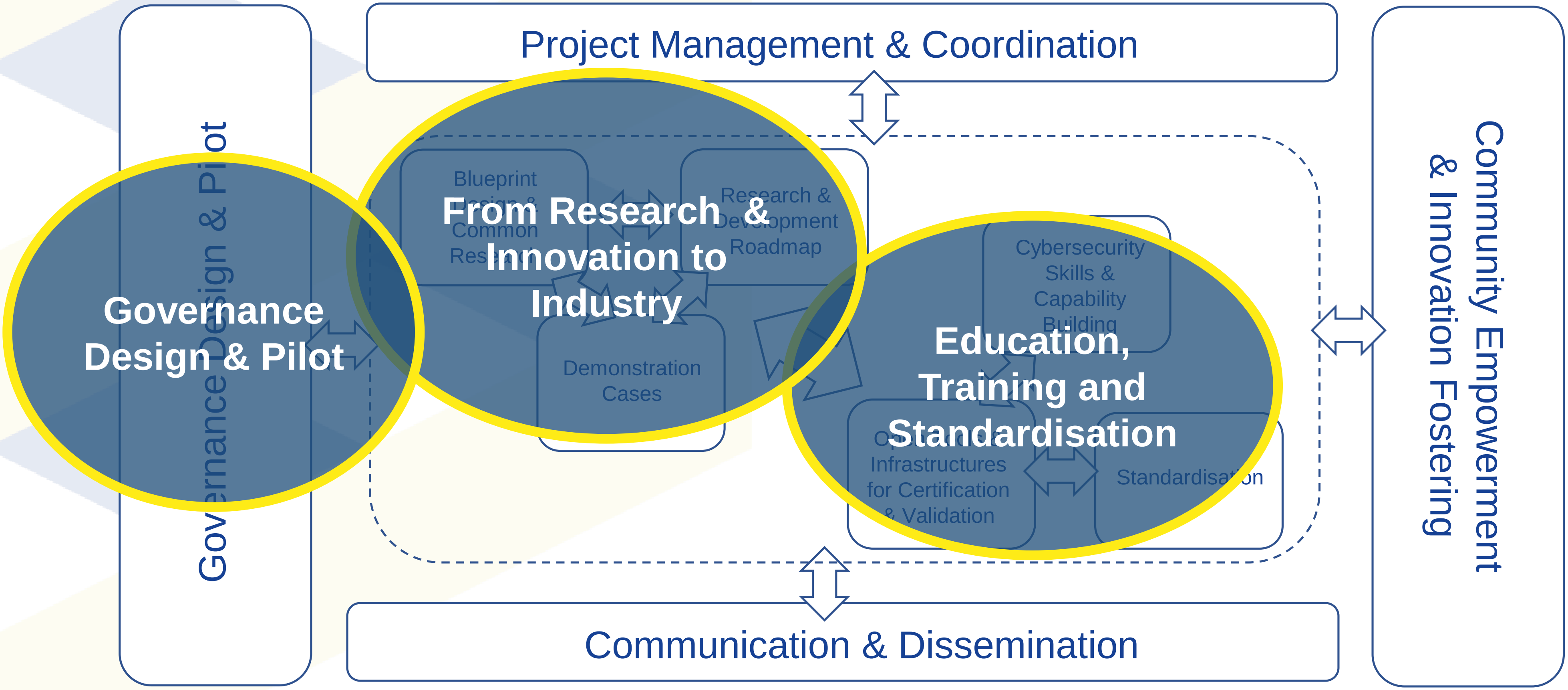
  ➢ E.g. Industry Groups, Local Governments, CERTs → not all the same level of formality as representatives of EC and MS

  ➢ May be different country by country (So regulation must allow this, e.g. sectoral vs regional)

➢ **Transparency** is a **key** element for facilitating **trust** in an **organization**.

Communication & Community Building

Cyber Security for Europe



Project Management & Coordination

Governance Design & Pilot

Governance Design & Pilot

From Research & Innovation to Industry

Blueprint Design & Common Research

Research & Development Roadmap

Demonstration Cases

Education, Training and Standardisation

Cybersecurity Skills & Capability Building

Open Tools & Infrastructures for Certification & Validation

Standardisation

Community Empowerment & Innovation Fostering

Communication & Dissemination

Results So Far: (Vertical) Application Use Cases

Available at cybersec4europe.eu

Requirements Analysis from **Vertical Stakeholders** (D4.1)

- Findings and recommendations from the engagement and consultation through a diverse set of approaches with vertical stakeholders (end users and industrial participants) to collect their requirements, to help define their important problems and to lay the foundation for the roadmap

Requirements Analysis of **Demonstration Cases** (D5.1)

- A comprehensive set of use cases and their requirements, covering the seven representative CyberSec4Europe demonstration cases.
- A thorough analysis with a rich set of functional and non-functional requirements (including security and privacy) that will guide research, technology development, and design, as well as the definition of the research roadmap.

Results So Far: Research

Available at cybersec4europe.eu

Common Framework Handbook 1 (D3.1)

- First version of CyberSec4Europe common framework.
- Architecture to encompass all of the proposed CyberSec4Europe functional components
- Common asset template
- First set of assets identified in WP3
- Mapping between the pilots requirements in WP5 and the assets available in WP3

Cross Sectoral Cybersecurity Building Blocks (D3.2)

Results So Far: Standards

Available at cybersec4europe.eu

Cybersecurity **Standardisation** Plan (D8.1)

- A snapshot of the activities that CyberSec4Europe partners are undertaking in the realm of standardisation and certification preparation.
- While some partners are clearly driving the efforts with SDOs and their committees, others are active participants in contributing content and feedback.

Results So Far: Governance

Available at cybersec4europe.eu

Governance Structure v1.0 (D2.1)

- Possible approaches to cybersecurity governance
- Comparison against the policy initiative proposed by the EC
- Proposal for a bottom-up Cybersecurity Governance Network
- First evaluation of the proposal via a small governance pilot

Case Pilot for Governance (D6.1)

- A review of the offerings of cybersecurity MOOCs in Europe, consisting of academic, continuous learning and cyber range courses.
- A definition of the quality assurance process for branding CyberSec4Europe MOOCs based on a list of criteria, both generic and cybersecurity specific.

Meet CyberSec4Europe
July 9, evening, Brussels

Cyber Security for Europe

Panel discussion with stakeholders, probably

- **Andreas Könen (**then**)** German **EU Presidency**
- **Tamara Tafra**, (current) Croatian **EU Presidency**
- …
- July 9, from 18.30 on
- Representation of the State of Hessen to the European Union
- Brussels, Rue Montoyer 21

Meet CyberSec4Europe December 9 - 11, Brussels

Cyber Security for Europe

2nd Concertation conference

- Together with the fellow pilots
- Topics (probably)
  - Governance
  - Demonstration cases
  - Stakeholder views
  - Research Road maps
  - …

- Representation of the State of Hessen to the European Union
- Brussels, Rue Montoyer 21

Cyber
Security
for Europe

cybersec4europe.eu
@cybersec4Europe
Kai.Rannenberg@m-chair.de

The Danish Hub for Cybersecurity as a national and industry and R&D hub

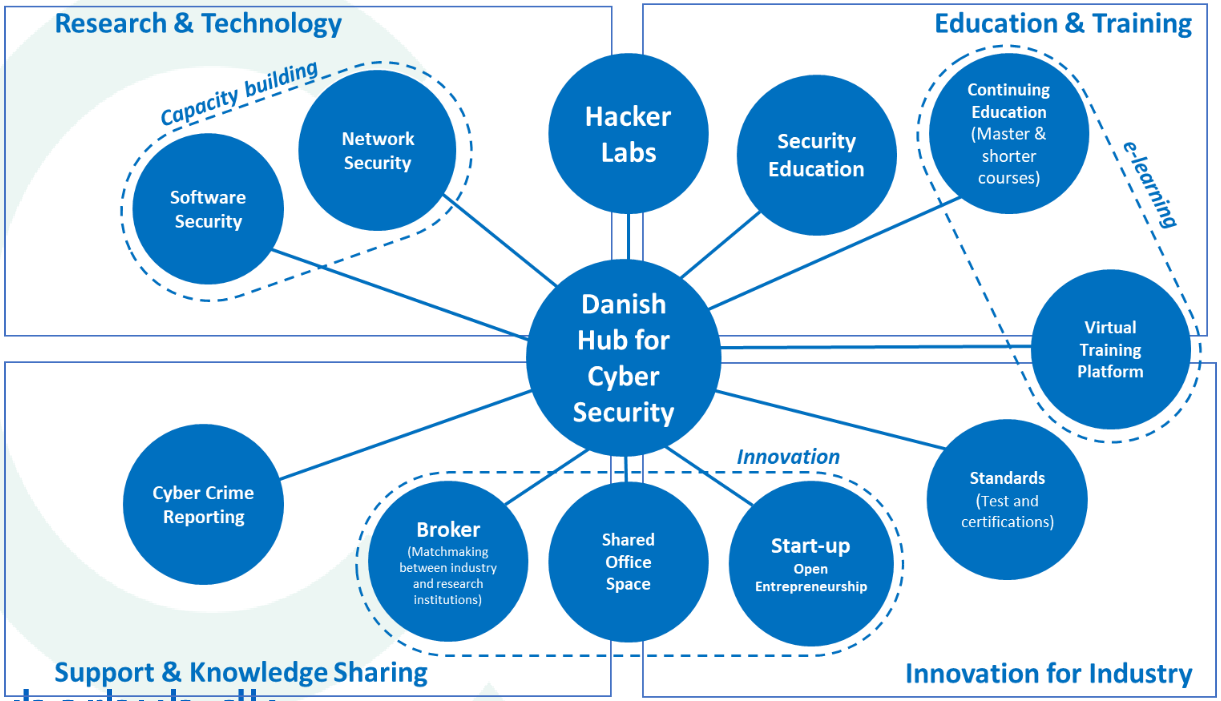
- All Danish universities; RTOs; Business academies; Industry networks.
- Strong collaboration with industry
- Strong collaboration with authorities
- Funded by The Danish Industry Foundation

Danish Academia, Danish Independent Research & Advisory Institutions and Industrial Networks

ALEXANDRA INSTITUTTET
AALBORG UNIVERSITY DENMARK
AARHUS UNIVERSITET
KØBENHAVNS UNIVERSITET
DTU
RUC
SDU
IT UNIVERSITY OF COPENHAGEN
infinit Innovationsnetværk for it
ERHVERVSAKADEMI AARHUS
FORCE TECHNOLOGY
CenSec CENTER FOR DEFENCE, SPACE & SECURITY
CBS COPENHAGEN BUSINESS SCHOOL HANDELSHØJSKOLEN
INDUSTRIENS FOND FREMMER DANSK KONKURRENCEEVNE The Danish Industry Foundation
DBI BRAND OG SIKRING
kea COPENHAGEN SCHOOL OF DESIGN AND TECHNOLOGY

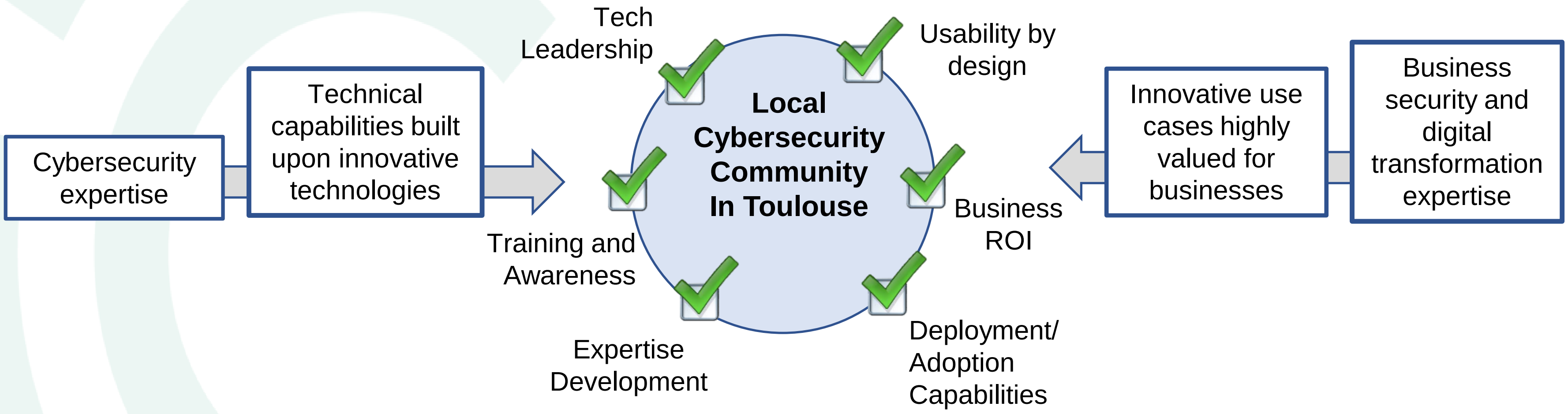
- Being launched as we speak

The Danish Hub for Cybersecurity as a National industry and R&D hub


Research & Technology
Capacity building
Network Security
Software Security
Hacker Labs
Security Education
Education & Training
Continuing Education (Master & shorter courses)
e-learning
Virtual Training Platform
Danish Hub for Cyber Security
Standards (Test and certifications)
Innovation
Cyber Crime Reporting
Broker (Matchmaking between industry and research institutions)
Shared Office Space
Start-up Open Entrepreneurship
Support & Knowledge Sharing
Innovation for Industry

- www.cyberhub.dk

OcSSImore/CHECK as a regional Community Hub of Expertise (Toulouse)

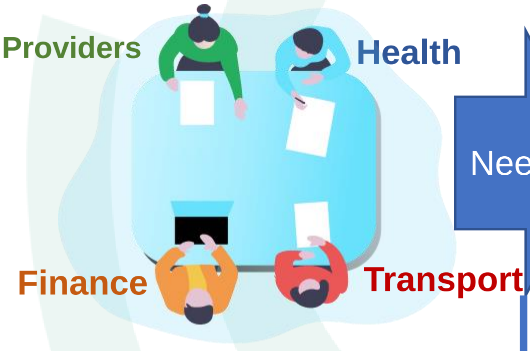

Cybersecurity expertise
Technical capabilities built upon innovative technologies
Tech Leadership
Usability by design
Local Cybersecurity Community In Toulouse
Training and Awareness
Business ROI
Expertise Development
Deployment/ Adoption Capabilities
Innovative use cases highly valued for businesses
Business security and digital transformation expertise

- Fostering a community providing a vision and the necessary expertise to create innovative, trustworthy digital services.
- Successful projects can thrive due to an agile governance model of case-by-case decisions on funding and innovation.

OcSSImore : Experience and achievements in 2019

1) Embodying a Cybersecurity R&I vision based on digital transformation needs
2) Merging several vertical sector visions to mature(*) critical and common cybersecurity needs and innovative business use-cases leveraging security
3) Driving the build of trans-sectorial innovations thus with a significant impact on economic development and local/national/EU digital market

1 **What critical uncovered security needs do we share?**



Needs

2 **As a vertical stakeholder, I want:**

→ To be able to continuously and efficiently **train my developers**, my ux designers, my managers, etc.… about cyber risks

→ To turn final **user authentication** into a simpler and stronger process which offers new (co-)business opportunities and leveraging user trust to grow

→ To better fight against globalized threat by being able to cooperate more efficiently with my fellow members and **sharing critical information** without transferring the ownership of my data

1 need interesting for OcSSImore = min 2 vertical stakeholders candidating to deploy a potential solution in its production environment and thus working together on the formalization of the need with a description of the ROI to reach

Quick Victory

3 **In 2018/2019, a first concrete realization is:**

→ A set of awareness training tools, https://digital-securite.ovh, https://empire.digital-securite.ovh, https://login.digital-securite.ovh,

→ Proof of concepts using FIDO2 and FranceConnect (EIDAS French platform) https://passeport.digital-securite.ovh, https://demo-fc.digital-securite.ovh

→ Experiments using secure multiparty computation to share information while keeping its secrecy for every involved party https://obsidian-project.eu

1 quick victory = a concrete realization which demonstrates the benefit in terms of security and/or user experience and achievable within 1 year

Project

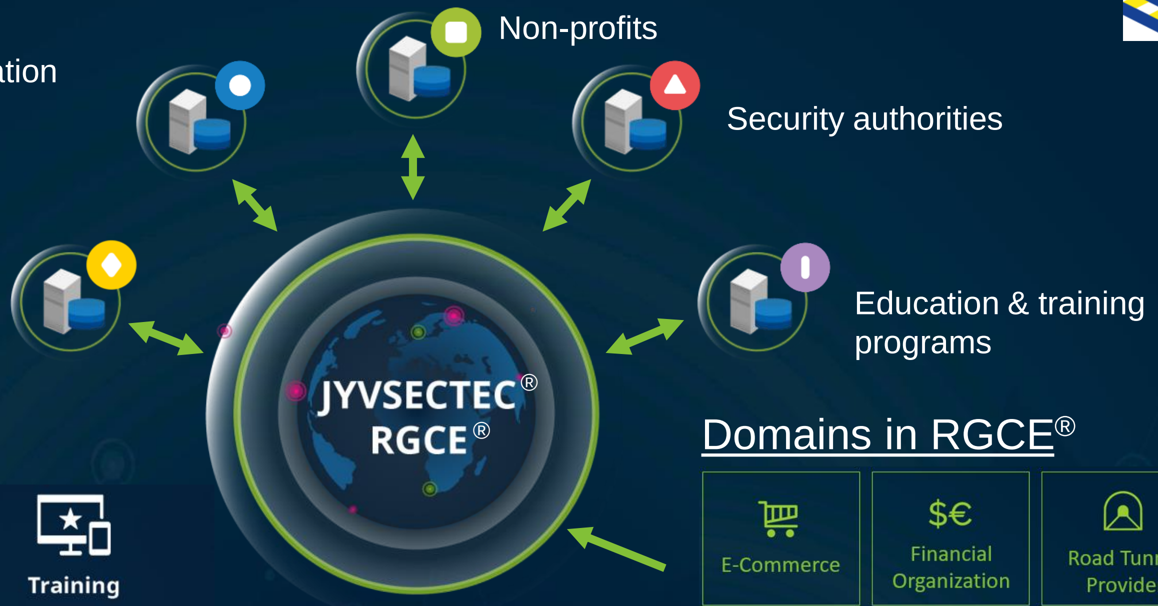
4 **Deploying a solution in production environment**

→ OcSSImore hasn't reached this maturity level yet

(*) common vocabulary and concepts to define the problem, common description of the limits of existing solutions, a consolidated analysis of the business ROI if the problem was solved,…

JYVSECTEC® National Cyber Range Ecosystem in Finland

Cyber Security for Europe



Services to Partners

FINCSC®
Certification mechanism for companies and communities to ensure business continuity.

Cyber exercises
Cyber security exercises in modern facilities with professional guidance.

Training
Diverse information and cyber security training for various fields of operation.

Testing
System and software security testing to identify the functional weaknesses and information security flaws.

Research
Research and development in separately funded projects or other joint research cooperation.

Consulting
Consulting in various fields of information and cyber security.

RGCE = Realistic Global Cyber Environment

Domains in RGCE®

E-Commerce	Financial Organization	Road Tunnel Provider
Electricity Company	Internet Service Provider	Cloud Service Provider
Healthcare Cyber Security	Governmental organizations	

https://jyvsectec.fi/rgce

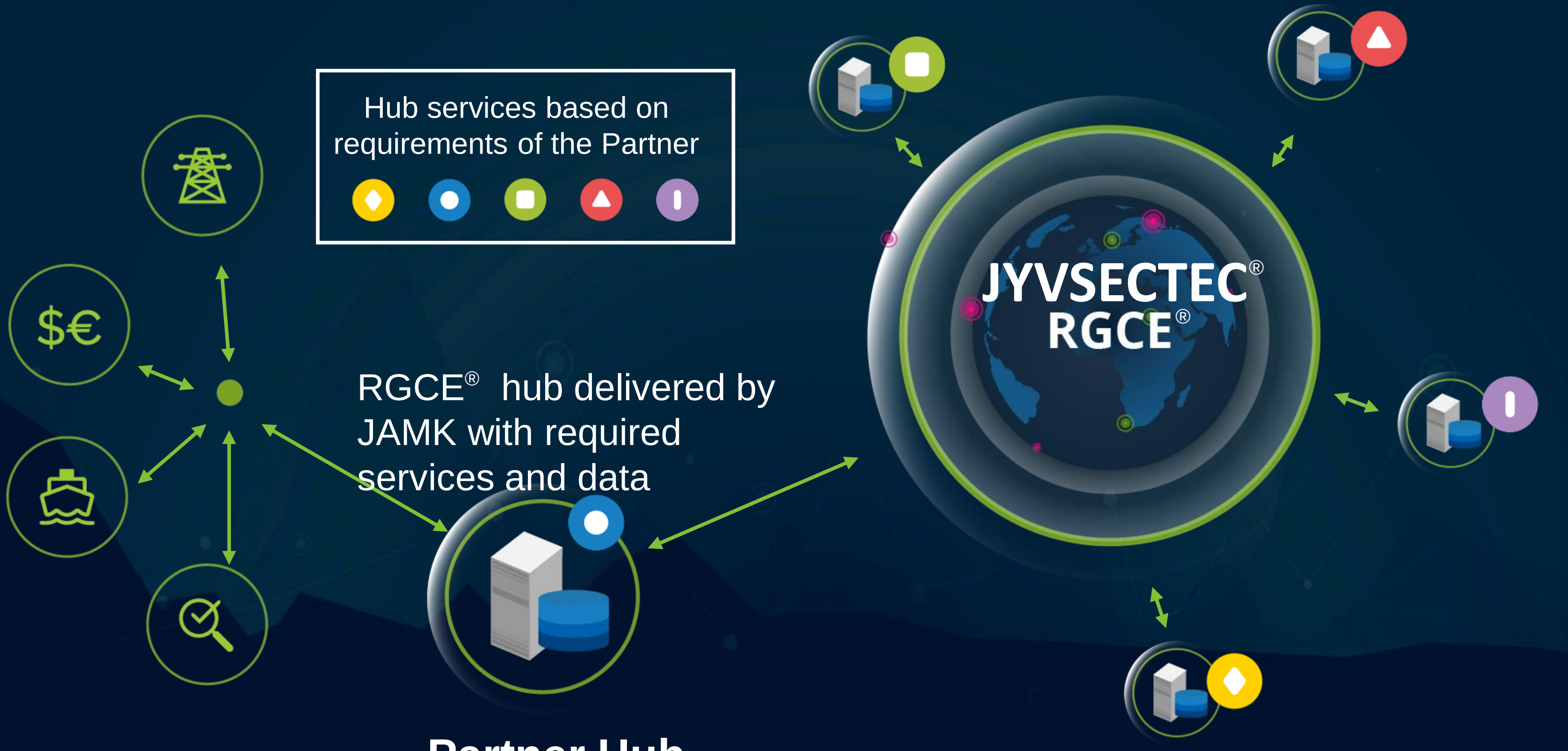
www.jyvsectec.fi

JYVSECTEC Jyväskylä Security Technology

jamk.fi Institute of Information Technology

JYVSECTEC® International Hub Concept

Cyber Security for Europe



Hub services based on requirements of the Partner

◆ ● ■ ▲ ❙

RGCE® hub delivered by JAMK with required services and data

Partner Hub

www.jyvsectec.fi

JYVSECTEC Jyväskylä Security Technology

jamk.fi Institute of Information Technology