Cyber Security for Europe

cyberwatching.eu

The European watch on cybersecurity & privacy

CyberSec4Europe

David Goodman, Trust in Digital Life
4 June 2019

Ensuring the competitiveness of Europe
Enabling European economic growth
while protecting European society

CyberSec4Europe is funded by the European Union under the H2020 Programme

Grant Agreement No. 830929

Cyber Ranges

Construct open tools and a common portable virtual lab

A lightweight cyber range from existing proven building blocks

Federated infrastructures for cyber range and testing

Map **existing cyber ranges**

Examine and provide **open tools**

Certification – methodologies, tools and infrastructures

Threat Intelligence

Enhancing the state of the art

for reliability, safety and privacy guarantees of security intelligence techniques based on artificial intelligence, machine learning and data analytics.

Investigating mechanisms

capable of interacting with Threat Intelligence Information Services to capture evidence of malware activity at an early stage.

Addressing research challenges

on log and event management, threat detection and security analytics with privacy-respecting big data analytics with the goal of enabling security intelligence in defensive systems, by ensuring the underpinning intelligence systems are fortified.

Certification

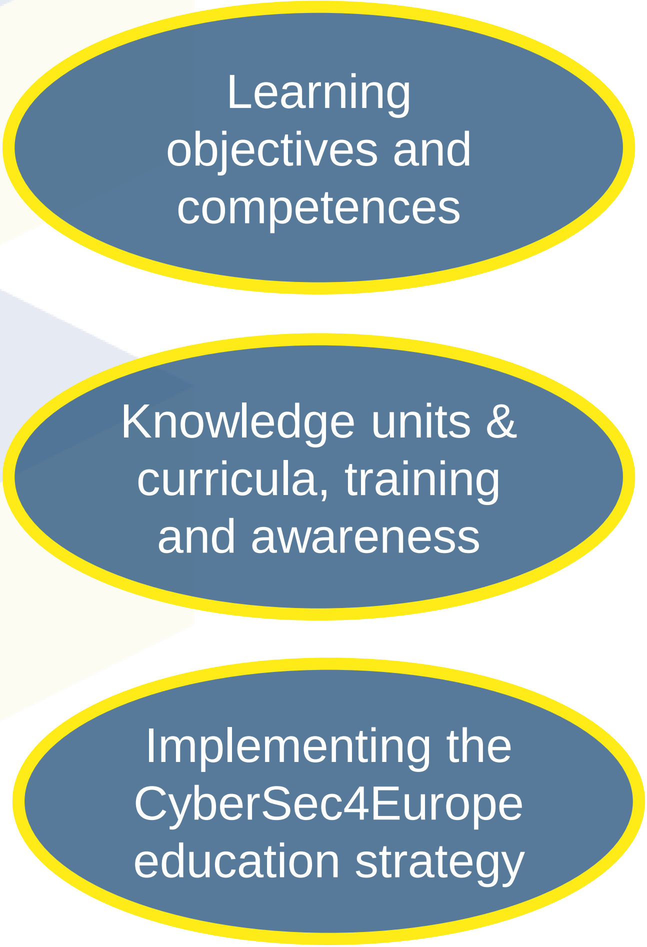
Methodologies, tools and infrastructures

To define governance and supporting services for security certification, with research, support, guidance and training for validation and certification of security properties of devices and systems for EU industry.

- Investigating certification for critical infrastructure components
- Aligning efforts with ENISA and ECSO framework policy work
- Cooperating with tools / services, standardization, conformity and validation
- Reducing time to certification of critical sector cyber physical systems
- Aligning with ECSO, on future certification and harmonisation
- Assessing the Cybersecurity Act, ISO27001 and GDPR

Cybersecurity Skills

To set an education and training framework and related instruments to support continuing education and lifelong learning in cybersecurity, organized to demonstrate the effectiveness of governance models and full transfer of pilot results to the future Centre’s operations.



Learning objectives and competences

required to develop and enhance cybersecurity skills for different profiles and roles.

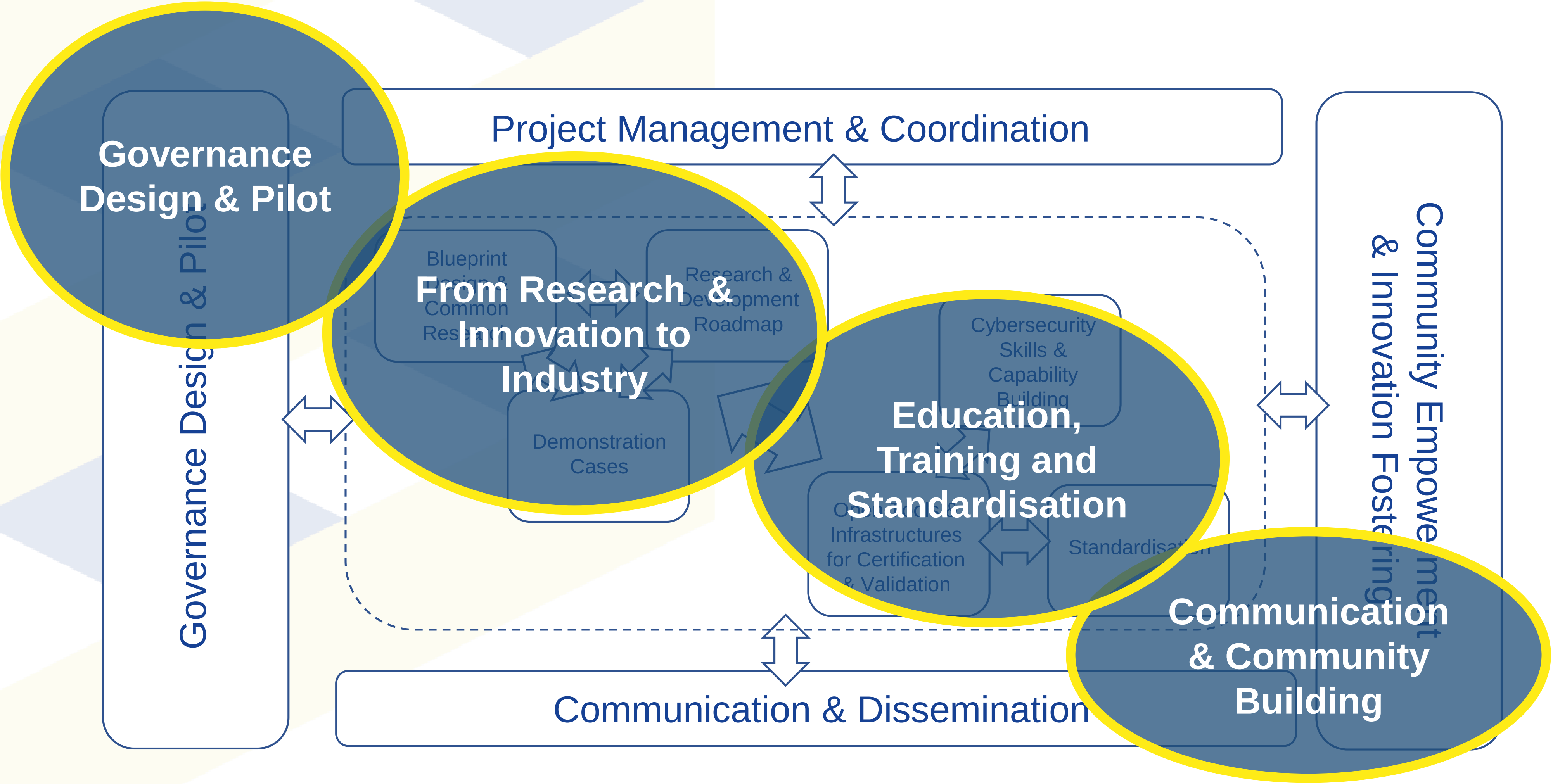
Knowledge units & curricula, training and awareness

to achieve objectives and competences, setting activities to apply and test such competencies.

Implementing the CyberSec4Europe education strategy

for citizens, students, and professionals promoting the project brand / guidelines / procedures to produce and consume content.

Piloting a Competence Network



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

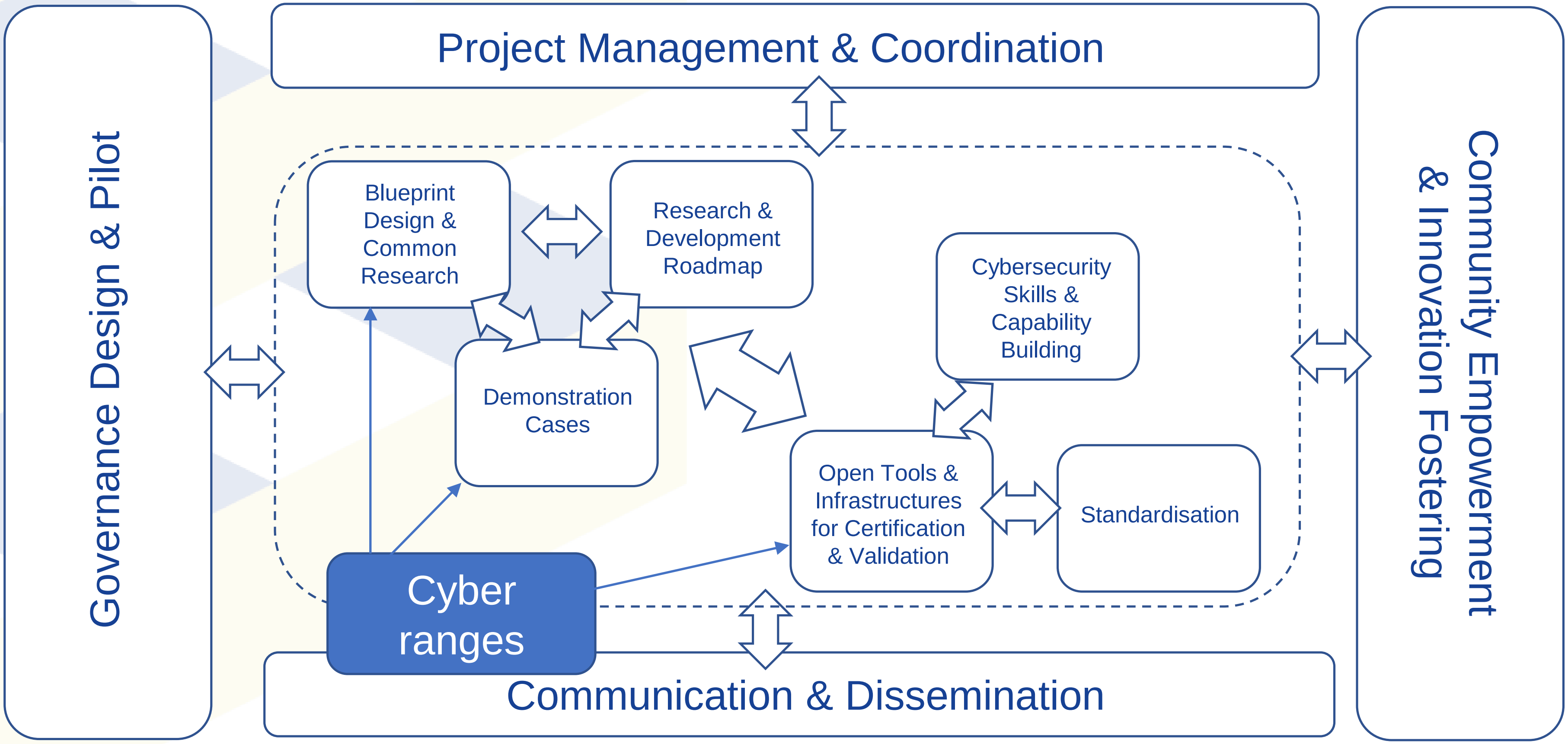
Governance Design & Pilot

From Research & Innovation to Industry

Education, Training and Standardisation

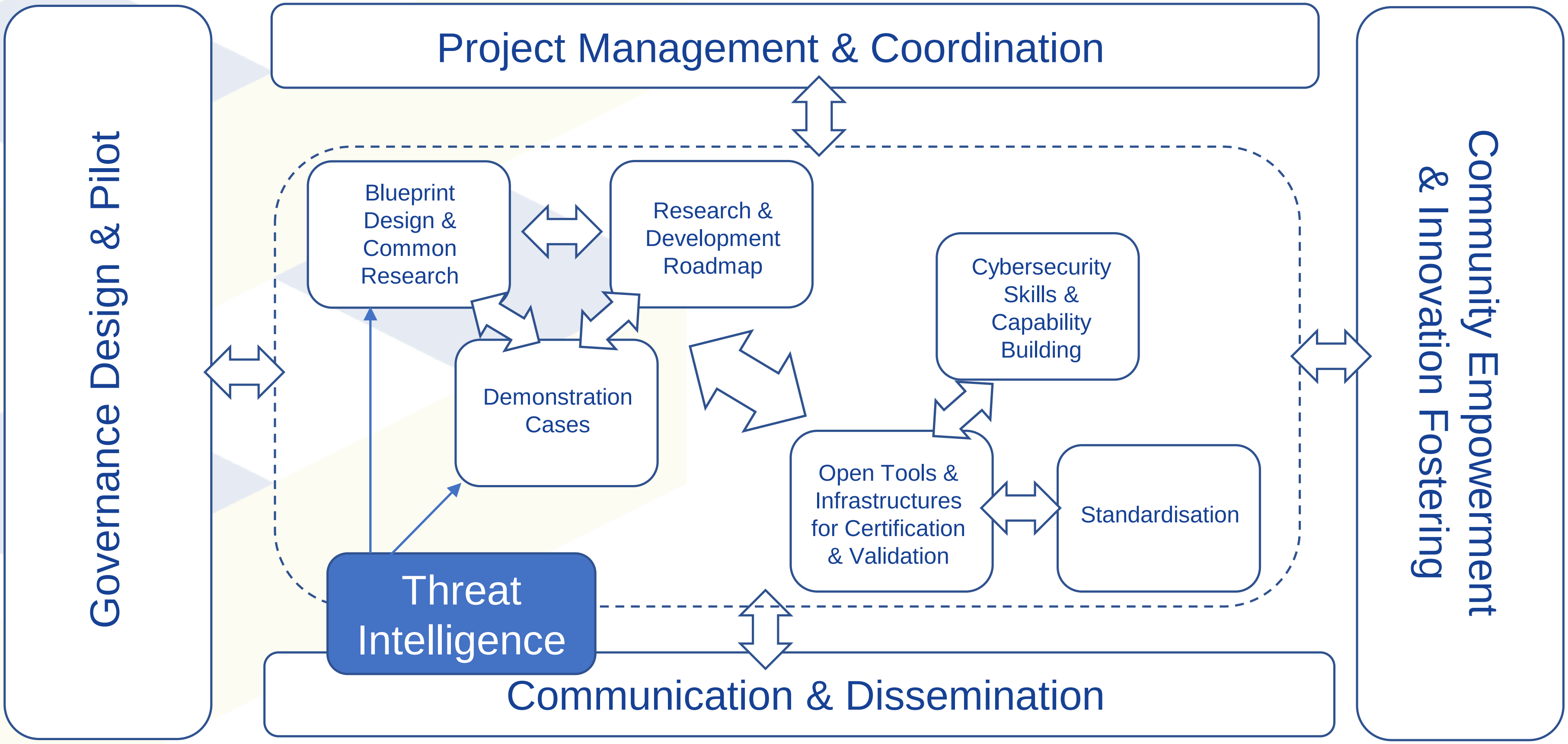
Communication & Community Building

Cyber Ranges


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

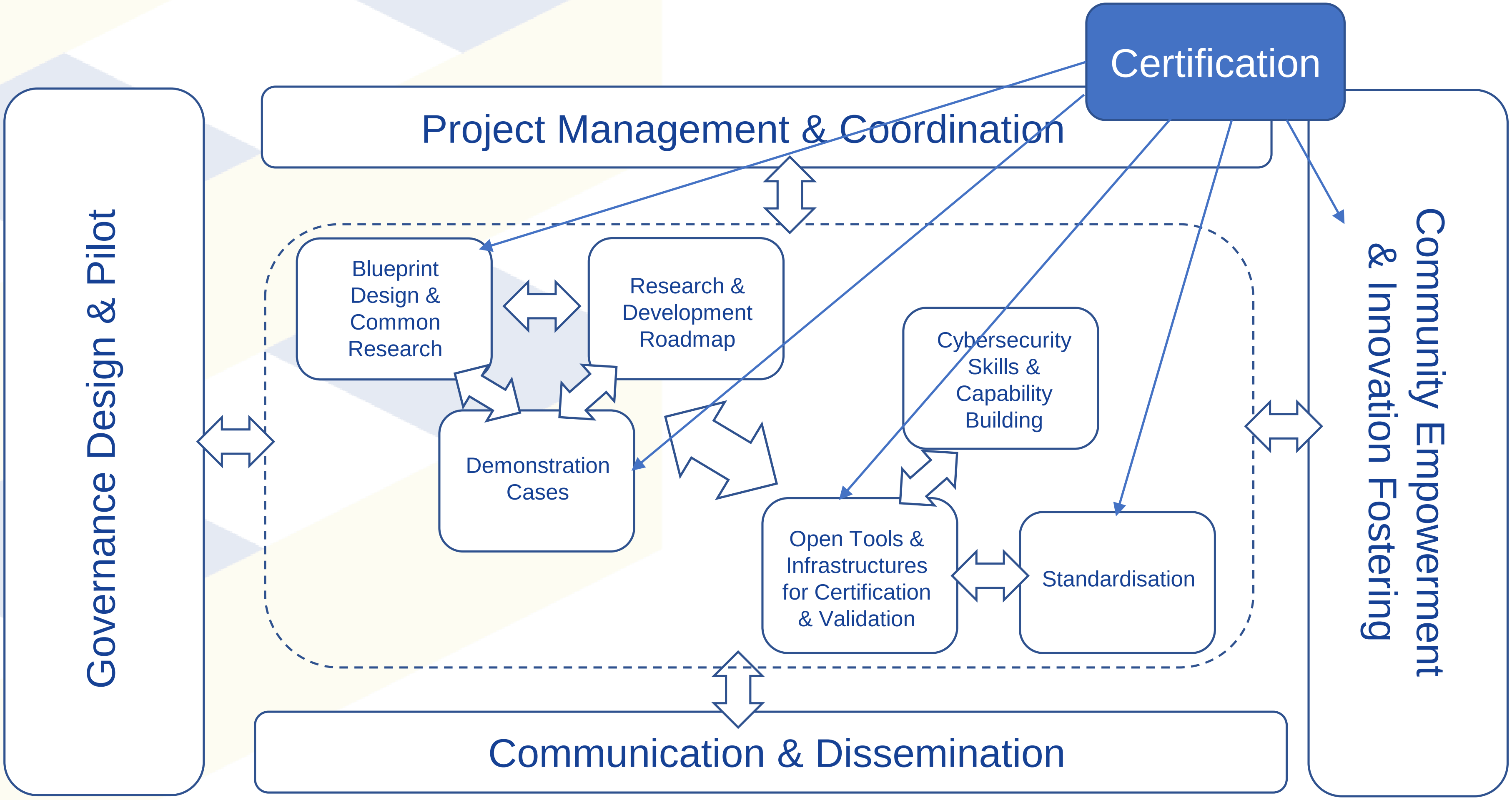
Threat Intelligence

Cyber Security for Europe

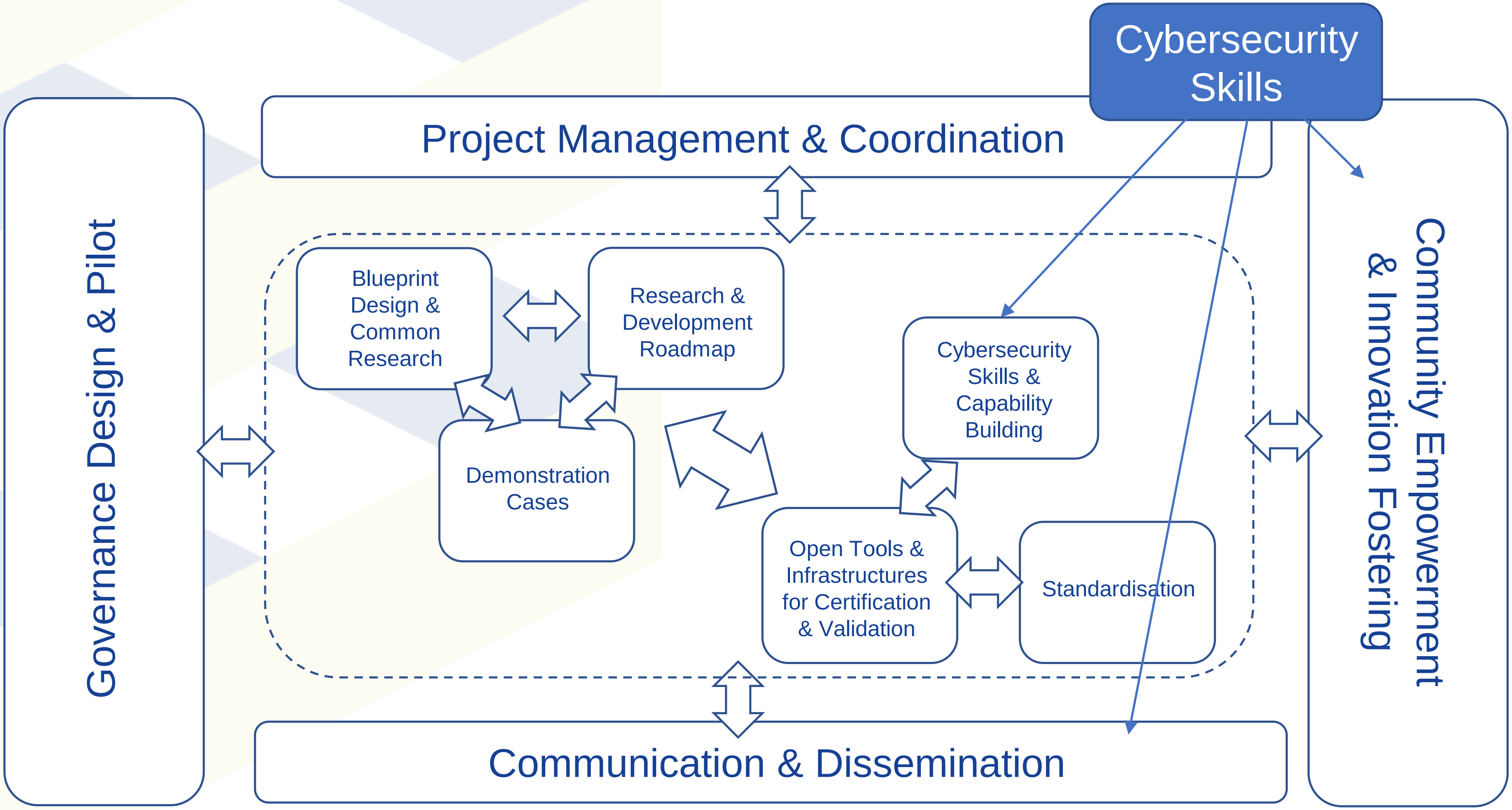

Governance Design & Pilot
Project Management & Coordination
Blueprint Design & Common Research
Research & Development Roadmap
Cybersecurity Skills & Capability Building
Demonstration Cases
Open Tools & Infrastructures for Certification & Validation
Standardisation
Threat Intelligence
Communication &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

Certification

Cyber Security for Europe


Certification
Project Management & Coordination
Governance Design & Pilot
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


Cybersecurity Skills
Project Management & Coordination
Governance Design & Pilot
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

Cyber Range Questions

Q1. Definition: No agreed definition exists between the four projects.**CyberSec4Europe** uses NIST and EDA definitions consisting of CRR, CSTR and CTER - a cyber range conceptually consists of all three

Q2: Benefits: readiness, resilience, training, development exercises for business, process and personnel

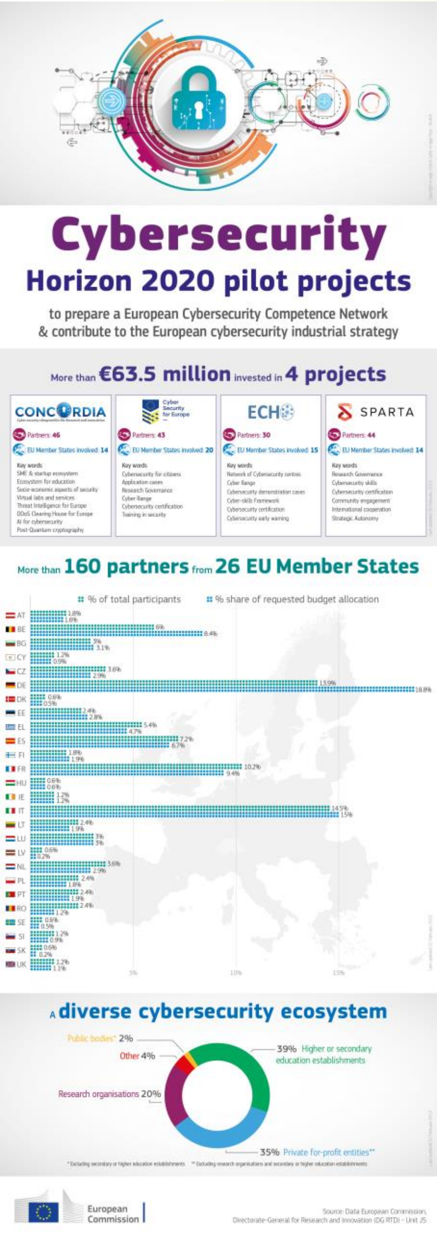
Q3: Existing: actual offering (scale, complexity, realism) varies globally. Larger IT vendors' cyber ranges, national cyber ranges providing commercial training, development, and research services and other university or state-owned cyber ranges **CyberSec4Europe** uses KYPO, RGCE

Q4: Technology: usually a virtualised infrastructure (networks, servers, end user workstations). For threat actor modelling, openly available pen-testing and red-teaming tools also custom-made tools and malware

Q5: Problems: technology – cloud environments; research – data set availability; economic: lack of understanding of benefits

Working Together Towards A Common Objective

Cyber Security for Europe



Cybersecurity

Horizon 2020 pilot projects

to prepare a European Cybersecurity Competence Network
& contribute to the European cybersecurity industrial strategy

More than €63.5 million invested in 4 projects

CONCORDIA	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 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	Key words Cybersecurity for citizens Application cases Research Governance Cyber Range Cybersecurity certification Training in security	Key words Network of Cybersecurity centres Cyber Range Cybersecurity demonstration cases Cyber-skills Framework Cybersecurity certification Cybersecurity early warning	Key words Research Governance Cybersecurity skills Cybersecurity certification Community engagement International cooperation Strategic Autonomy

More than 160 partners from 26 EU Member States

	% of total participants	% share of requested budget allocation
AT	1.8%	1.6%
BE	6%	8.4%
BG	3%	3.1%
CY	1.2%	0.9%
CZ	3.6%	2.9%
DE	13.9%	18.8%
DK	0.6%	0.5%
EE	2.4%	2.8%
EL	5.4%	4.7%
ES	7.2%	6.7%
FI	1.8%	1.9%
FR	10.2%	9.4%
HU	0.6%	0.6%
IE	1.2%	1.2%
IT	14.5%	15%
LT	2.4%	1.9%
LU	3%	3%
LV	0.6%	0.2%
NL	3.6%	2.9%
PL	2.4%	1.8%
PT	2.4%	1.9%
RO	2.4%	1.2%
SE	0.6%	0.5%
SI	1.2%	0.9%
SK	0.6%	0.2%
UK	1.2%	1.1%

A diverse cybersecurity ecosystem

Public bodies*	2%
Other	4%
Research organisations	20%
Higher or secondary education establishments	39%
Private for-profit entities**	35%

* Excluding secondary or higher education establishments ** Excluding research organisations and secondary or higher education establishments

European Commission

Source: Data European Commission, Directorate-General for Research and Innovation (DG RTD) - Unit J5

ECHO

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

SPARTA

Cyber Competence Network

Cyber Security for Europe

A European network of cybersecurity centres of excellence

Cyber Security for Europe

cyberwatching.eu

The European watch on cybersecurity & privacy

Additional Material

Q1: What is the definition of cyber ranges that the four of them have agreed upon?

Cyber Security for Europe

No agreed definition exists between the four projects.

NIST [1] defines cyber ranges as interactive, simulated representations of an organization's local network, system, tools, and applications that are connected to a simulated Internet level environment. They provide a safe, legal environment to gain hands-on cyber skills and a secure environment for product development and security posture testing

EDA [2] defines cyber range as: a multipurpose environment in support of three primary processes: knowledge development, assurance and dissemination. It consists of three complementary functionality packages:

- **Cyber Research Range (CRR)** A facility where in close cooperation with research centres, private sector, academic institutions knowledge development (research) takes place. Where newly gained knowledge can be utilised in new products, processes and/or services (development). A facility where e.g. ICT, network information & architecture (NII) in a variety of configurations and circumstances can be analysed. Currently used systems can be analysed as well.
- **Cyber Simulation & Test Range (CSTR)** A facility within the cyber range where the current ICT-reality of a specific network configuration can be simulated, in which possible effects of cyber operations can be tested. The CSTR enables experimental testing of cyber capabilities in a realistic manner, but in a safe, isolated setting.
- **Cyber Training & Exercise Range (CTER)** In order to achieve the necessary growth and sustainability in human capital, a state-of-the-art training & exercise functionality is needed. Modeling & simulation is a valuable asset where knowledge and skills concerning cyber capabilities and cyber operations can be trained and tested. A setting where cyber operators under simulated circumstances can be trained for utilizing cyber capabilities.

A cyber range conceptually consists of all three

Q2: Benefits of utilising cyber range

for companies/organizations in cybersecurity exercise

Cyber Security for Europe

Cybersecurity exercise is a powerful tool for enhancing an organization’s readiness and resilience against modern cyber threats

The complexity of the enterprise’s IT environment has created the need to conduct larger scale cybersecurity exercises to train personnel and develop business and IT processes to handle different cyber incidents

Cybersecurity exercises provide opportunities for organisations to demonstrate critical capabilities

- Exercises reveal how effectively they integrate people, processes, and technology to protect their critical information, services, and assets

Q3: What are the existing cyber ranges

in the public and private sectors?

As cyber range is not strictly defined, organisations / companies providing or operating cyber ranges declare their offering to be a cyber range, thus the actual offering (scale, complexity, realism) varies globally

- A pre-defined simple and limited environment to provide infrastructure for Capture The Flag (CTF), e.g. a single virtual machine. Network accessible but limited environment to perform CTF exercises.
- Locally accessible infrastructure, participants must utilize their own laptops and actual work emails and systems; no malware can be used.
- Locally accessible complex and large scale infrastructure, where all equipment and devices are provided by the cyber range vendor/operator, which allows real malware running without fear of malware leaking to Internet or exercising parties business network

Existing cyber ranges vary from larger IT vendors (e.g. IBM, Cisco or Palo Alto networks) cyber ranges to national cyber ranges providing commercial training, development, and research services (Finnish JYVSECTEC's RGCE) and other university or state-owned cyber ranges (Czech KYPO or Swedish CRATE)

Q4: What technologies are they using?

It varies, but usually the environment is run on a virtualised infrastructure (networks, servers, end user workstations)

Depending on the cyber range, the usage of commercial solutions varies, but almost all cyber ranges utilise open source solutions widely to provide training and exercise environments

- These solutions vary from basic information security controls (IDSs, firewalls, endpoint-protections (AVs) to more advanced machine learning / data analytical solutions.
- In addition, many of the traditional IT infrastructure solutions (Windows domains, proxies, DNS, etc.) are used to create realistic organisational environments for exercises
- For threat actor modelling, many cyber ranges utilise openly available pen-testing tools and red-teaming tools but also different custom-made tools and malware to represent real cyber attacks

Q5: What are the open problems

(technological, research, policy, economical oriented) for their future facilitation, exploitation and sustainability?

Technological

Companies and organizations are increasingly utilising cloud services, and providers are usually focused on global actors such as Amazon, Apple, Microsoft, Facebook, Google, Alibaba. Modelling these vendors' services realistically is non-trivial

Increasingly security control mechanisms are run on cloud environments for performing the analytics and computing required

Research

For example data analytics/deep-learning on cybersecurity requires suitable data sets not openly available

Economic

Organisations should increase cyber range usage in their annual business continuity plans to test, develop and verify preparedness against modern threats

Unfortunately many organizations have not identified the need to exercise, often through lack of understanding of the benefits, usually seen as training for technical personnel, whereas they should be seen as tools to develop the whole organization’s capabilities on handling cyber attacks and preparing personnel against major incidents.