Cybersecurity in Horizon Europe & Digital Europe

@Shaping the future of cybersecurity - Priorities, challenges and funding opportunities for a more resilient Europe

13 July 2021

Monika Lanzenberger

European Commission
DG CNECT.H1 Cybersecurity Technology and Capacity Building

THE EU'S CYBERSECURITY STRATEGY FOR THE DIGITAL DECADE

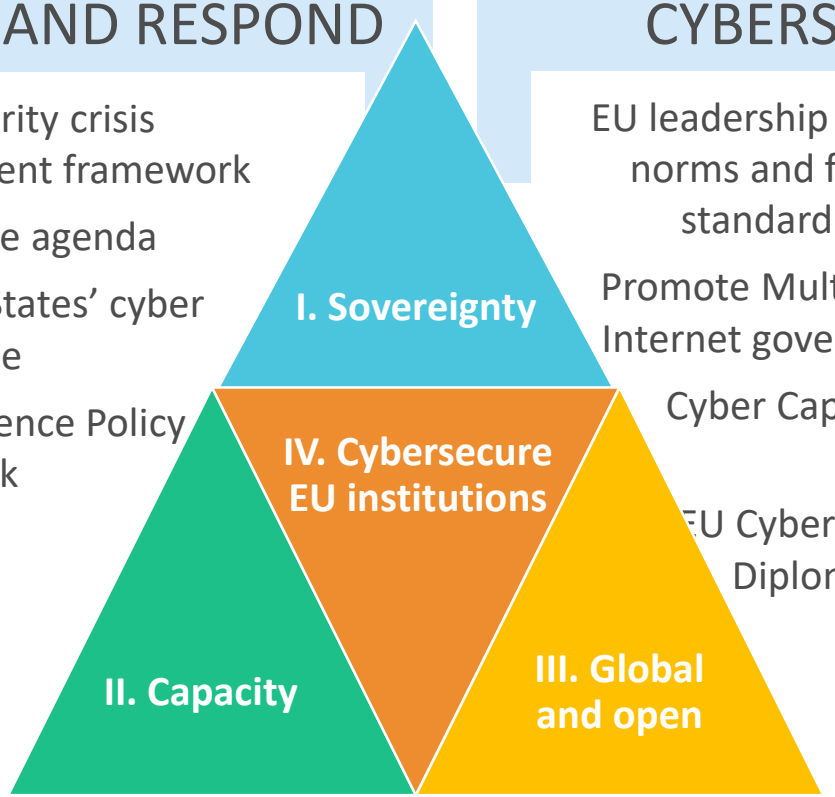
The EU's Cybersecurity Strategy for the Digital Decade (16.12.2020); 3 instruments (regulatory, investment, policy initiatives) 3 to three pillars

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

Project Funding – Digital Europe and Horizon Europe

2021-2022

European Commission

Cybersecurity in Horizon Europe 2021-2022

Resilient digital infrastructures and interconnected systems

- Dynamic business continuity and recovery methodologies
- Monitoring of threats and intrusion detection

Hardware, software and supply chain security

- Improved security in open-source and open-specification hardware for connected devices
- Trustworthy methodologies, tools and data security for dynamic testing

Cybersecurity and disruptive technologies

- AI for cybersecurity reinforcement
- Transition towards Quantum-Resistant Cryptography

Smart and quantifiable security assurance & certification across Europe

- Agile certification of ICT products, ICT services and ICT processes

Human-centric security, privacy and ethics

- Technologies for cross-border federated computation in Europe involving personal data

Expected impact of the Cybersecurity Actions (1/2)

4. Destination – Increased Cybersecurity

"*Increased cybersecurity and a more **secure online** environment by developing and using effectively EU and Member States' **capabilities** in digital technologies supporting protection of data and networks aspiring to **technological sovereignty** in this field, while respecting **privacy** and other **fundamental rights**; this should contribute to secure services, processes and products, as well as to robust digital infrastructures capable to resist and counter **cyber-attacks and hybrid threats**.*" (Strategic Plan 2021-2024)

Expected impact of the Cybersecurity Actions (2/2)

Proposals should contribute to the achievement of one or more of the following impacts:

- Strengthened EU cybersecurity capacities and European Union sovereignty in digital technologies
- More resilient digital infrastructures, systems and processes
- Increased software, hardware and supply chain security
- Secured disruptive technologies
- Smart and quantifiable security assurance and certification shared across the EU
- Reinforced awareness and a common cyber security management and culture

Cybersecurity in Horizon Europe 2021-2022

What we are looking for: (the big picture)

- Contribution to the implementation of Union policies: NIS Directive, EU Cybersecurity Act, EU Cybersecurity Strategy, GDPR and future e-Privacy Regulation.
- Building on past and ongoing activities: Horizon 2020 projects (incl. pilots) & ENISA
- Alignment to the objectives of the Cybersecurity Competence Centre and Network of National Coordination Centres (Regulation (EU) 2021/887) as relevant
- Complementarity with other actions under Horizon Europe (cluster #4: *Digital, Industry & Space*) and the Digital Europe Programme
- Potential input (as relevant) into the operational work on preparedness and response of the Joint Cyber Unit

Cybersecurity Topics in 2021

Resilient digital infrastructures and interconnected systems

HORIZON-CL3-2021-CS-01-01: Dynamic business continuity and recovery methodologies based on models and prediction for multi-level Cybersecurity

Hardware, software and supply chain security

HORIZON-CL3-2021-CS-01-02: Improved security in open-source and open-specification hardware for connected devices

Cybersecurity and disruptive technologies

HORIZON-CL3-2021-CS-01-03: AI for cybersecurity reinforcement

Human-centric security, privacy and ethics

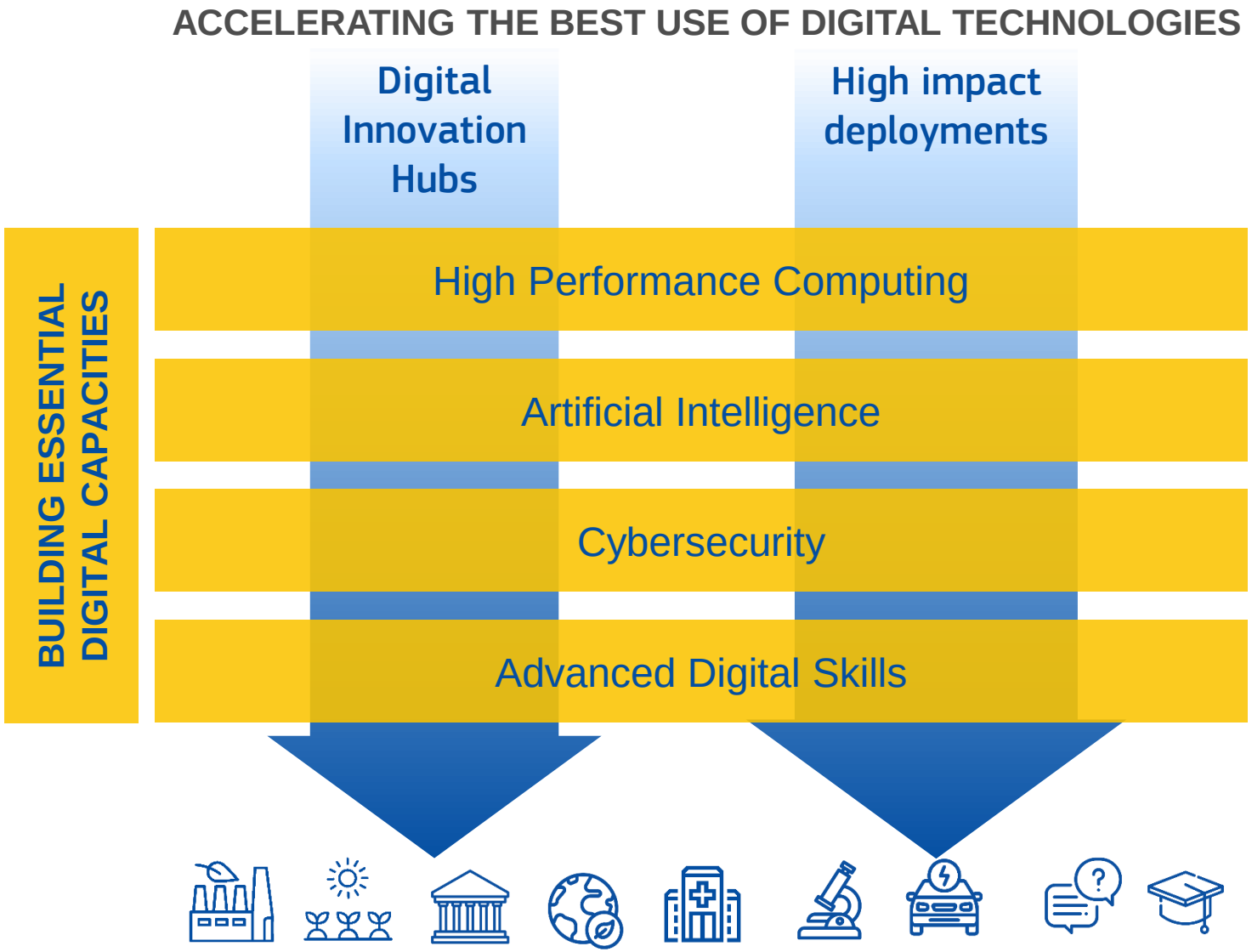
HORIZON-CL3-2021-CS-01-04: Scalable privacy-preserving technologies for cross-border federated computation in Europe involving personal data

Overview & Timing

- Submission Deadline: **21/10/2021** for the 2021 topics in Cyber
- Successful proposals to be notified: March 2022 (tentatively)
- Indicative Time to Grant Signature: 8 months (June 2022)

TOPIC	Title	Type of Action	Open Date	Deadline	Budget	Recommended budget per proposal
CL3-2021-CS-01-01	Dynamic business continuity and recovery methodologies based on models and prediction for multi-level Cybersecurity	RIA	30/06/2021	21/10/2021	€ 21,50M	€ 3M – 5M
CL3-2021-CS-01-02	Improved security in open-source and open-specification hardware for connected devices	RIA	30/06/2021	21/10/2021	€ 18M	€ 3M – 5M
CL3-2021-CS-01-03	AI for cybersecurity reinforcement	RIA	30/06/2021	21/10/2021	€ 11M	€ 3M – 4M
CL3-2021-CS-01-04	Scalable privacy-preserving technologies for cross-border federated computation in Europe involving personal data	RIA	30/06/2021	21/10/2021	€ 17M	€ 3M – 5M

Digital Europe programme structure



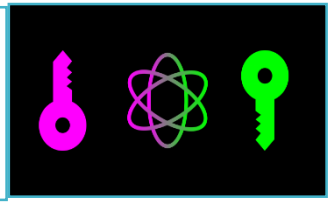
European Commission

DIGITAL EUROPE (2021 – 2027)
Initial funding priorities (draft)

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, …)

Other related Cybersecurity activities

European Cybersecurity Competence Centre and Network

Joint Cyber Unit

Cybersecurity Act - Certification

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:

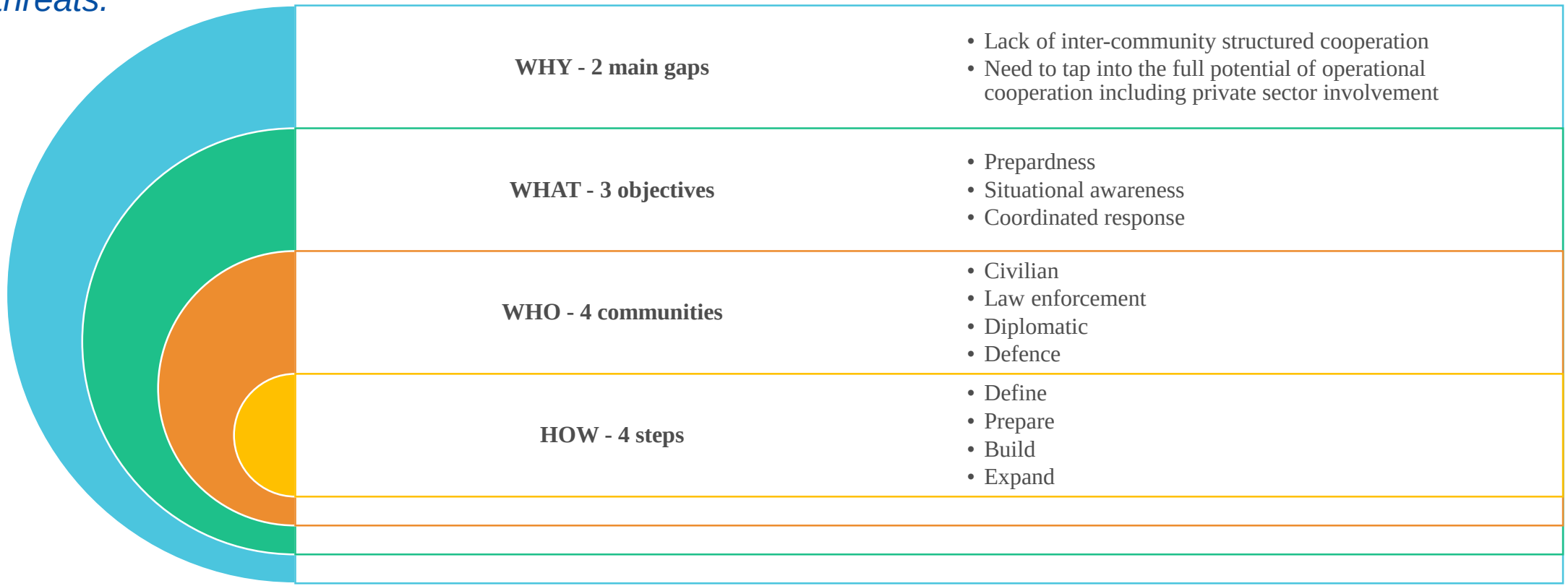
- Nominated by Member States as the national contact point
- Objective: national capacity building and link with existing initiatives
- National Coordination Centres may receive funding
- National Coordination Centres may pass on financial support

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

The Joint Cyber Unit

A virtual and physical platform for cooperation for the different cybersecurity communities in the EU, with a focus on operational and technical coordination against major cross border cyber incidents and threats.



European Commission

Cybersecurity Act - Certification - State of play

Cybersecurity Act

- Entry into force June 2019

Advisory groups

- ECCG - established
- SCCG - established

Candidate Schemes

- “SOG-IS MRA” /EUCC/ pending Implementing Act
- Cloud Scheme
- Request for 5G scheme

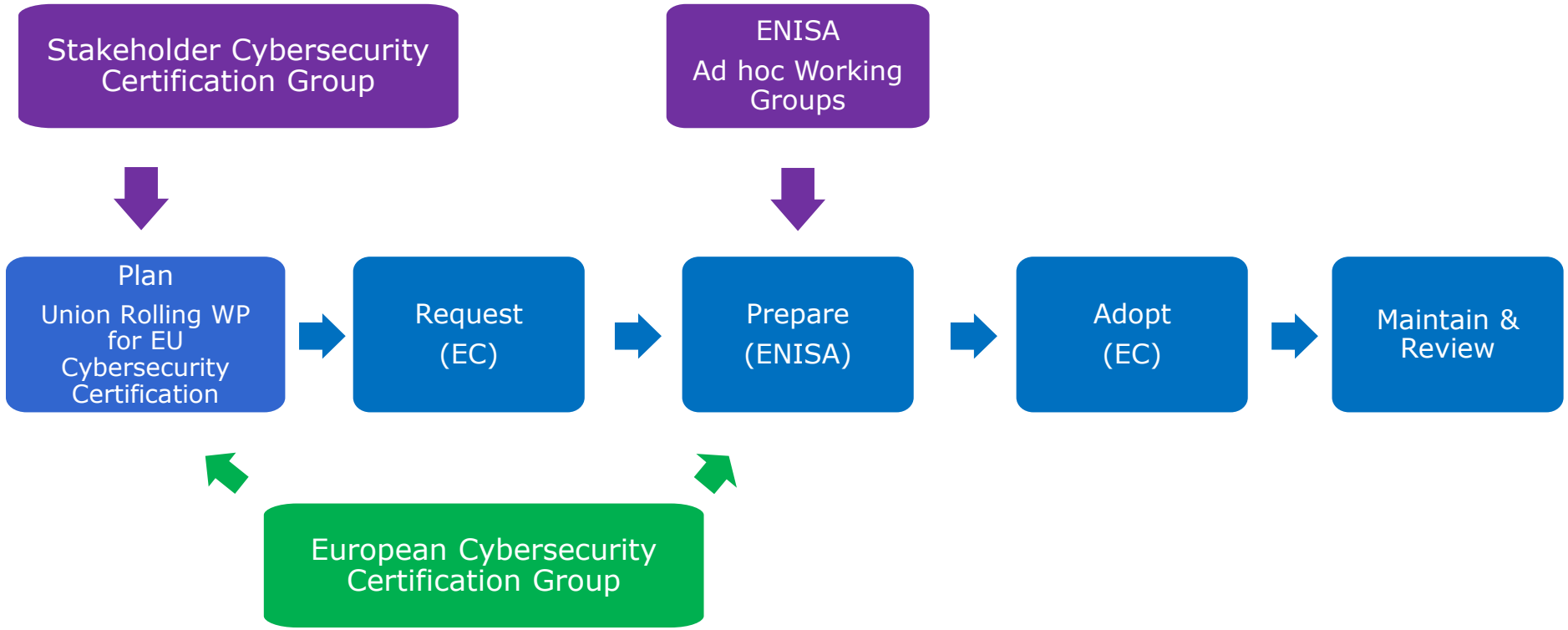
Union Rolling Work Programme for European Cybersecurity certification

- Pending Publication (2021)

The European Cybersecurity Certification Framework - features

- **One Framework, many schemes**
- **Voluntary** nature: unless specified in future EU/national rules
- **Scope:** Products, services, or processes
- Inclusive and transparent **governance** processes
- Use of international **standards**, as much as possible
- Each scheme can contain **specific provisions** on: re-certification, vulnerability handling and disclosure, provision of updates, surveillance, peer review
- Three levels of **assurance** to be defined on basis of risk of intended use

The lifecycle of a European Cybersecurity Certification Scheme



Further reading

- Horizon Europe Work Programme Cluster 3 – Civil Security for Society : https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/wp-call/2021-2022/wp-6-civil-security-for-society_horizon-2021-2022_en.pdf
- Digital Europe: https://digital-strategy.ec.europa.eu/en/activities/digital-programme
- The European Cybersecurity Compentence Centre and Network: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre and the Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres: https://eur-lex.europa.eu/eli/reg/2021/887/oj
- Recommendation on building a Joint Cyber Unit: https://digital-strategy.ec.europa.eu/en/library/recommendation-building-joint-cyber-unit

Thank you

European Commission

Annex

HORIZON-CL3-2021-CS-01-01: Dynamic business continuity and recovery methodologies based on models and prediction for multi-level Cybersecurity

European Commission

HORIZON-CL3-2021-CS-01-01: Dynamic business continuity and recovery methodologies based on models and prediction for multi-level Cybersecurity (1/3)

Expected Outcome

Projects are expected to contribute to all of the following expected outcomes:

- Advanced self-healing disaster recovery and effective business continuity in critical sectors (e.g. energy, transportation, health);
- Enhanced mechanisms for exchange of information among relevant players;
- Better disaster preparedness against possible disruptions, attacks and cascading effects;
- Better business continuity covering two or more sectors.

HORIZON-CL3-2021-CS-01-01: Dynamic business continuity and recovery methodologies based on models and prediction for multi-level Cybersecurity (2/3)

Scope

- New methodologies, services and tools for accelerating the self-recovery after an attack
- Beyond the state-of-the-art in developing and validating AI-based self-healing, effective business continuity and disaster recovery in real-world scenarios for two or more business sectors
- Collaboration and data sharing between different security actors, dynamic execution of disruption recovery and business continuity processes
- Real-time personalised technical assistance, share information and alerts with relevant stakeholders
- NIS Directive: critical sectors (e.g. energy, transportation, health) and telecommunication networks
- Satisfy needs of the end-users and support daily tasks, address human factors, Social Sciences and Humanities expertise, SME participation encouraged

HORIZON-CL3-2021-CS-01-01: Dynamic business continuity and recovery methodologies based on models and prediction for multi-level Cybersecurity (3/3)

- Expected EU contribution per project: EUR 3M – 5M
- Indicative topic budget: EUR 21,50M
- Type of Action: RIA (Research & Innovation Action)
- Technology Readiness Level: TRL4 (by the end of the project)

- Link to Participant Portal:

https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2021-cs-01-01

European Commission

HORIZON-CL3-2021-CS-01-02: Improved security in open-source and open-specification hardware for connected devices

European Commission

HORIZON-CL3-2021-CS-01-02: Improved security in open-source and open-specification hardware for connected devices (1/3)

Expected Outcome

To increase the security of connected devices (IoT), in particular with developments in open hardware, by embedding the cybersecurity dimension within their lifecycle management.

Projects are expected to contribute to some of the following expected outcomes:

- Mitigating **security threats** of open source hardware for connected devices
- Providing **formal verification** of open hardware
- Effective management of **cybersecurity patches** in restricted environments, such as IoT.
- Effective **security audits** of open source hardware, embedded software and other security-relevant aspects of connected devices
- Effective mechanisms for **inventory management**, detection of insecure components and **decommissioning**.
- Methods for **secure authentication** and **secure communication** for connected devices in restricted environments such as IoT devices

HORIZON-CL3-2021-CS-01-02: Improved security in open-source and open-specification hardware for connected devices (2/3)

Scope

To address the challenge of cybersecurity in the lifecycle management of connected devices in the Open Source collaborative development environment.

- Proposals are expected to **develop** within the following research activities:
  - **verifiable implementations** of cryptographic solutions, authentication schemes, and, as relevant, software libraries that implement them securely in operating systems;
  - mechanisms to mitigate **hardware-related** security **vulnerabilities**
  - security **auditing** & security **testing** in restricted environments;
  - verification methods for secure **firmware updates**, secure **software patching, security upgrading** within the life cycle (bootstrapping, commissioning, operational, upgrade etc.)
  - **multi-factor authentication** hardware and software solutions.

Participation of SMEs is strongly encouraged

HORIZON-CL3-2021-CS-01-02: Improved security in open-source and open-specification hardware for connected devices (3/3)

- Expected EU contribution per project: EUR 3M – 5M
- Indicative topic budget: EUR 18M
- Type of Action: RIA (Research & Innovation Action)
- Technology Readiness Level: TRL4 (by the end of the project)
- Topic specific condition: Gender dimension **not** mandatory

- Link to Participant Portal:

https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2021-cs-01-02

HORIZON-CL3-2021-CS-01-03:
AI for cybersecurity reinforcement

European Commission

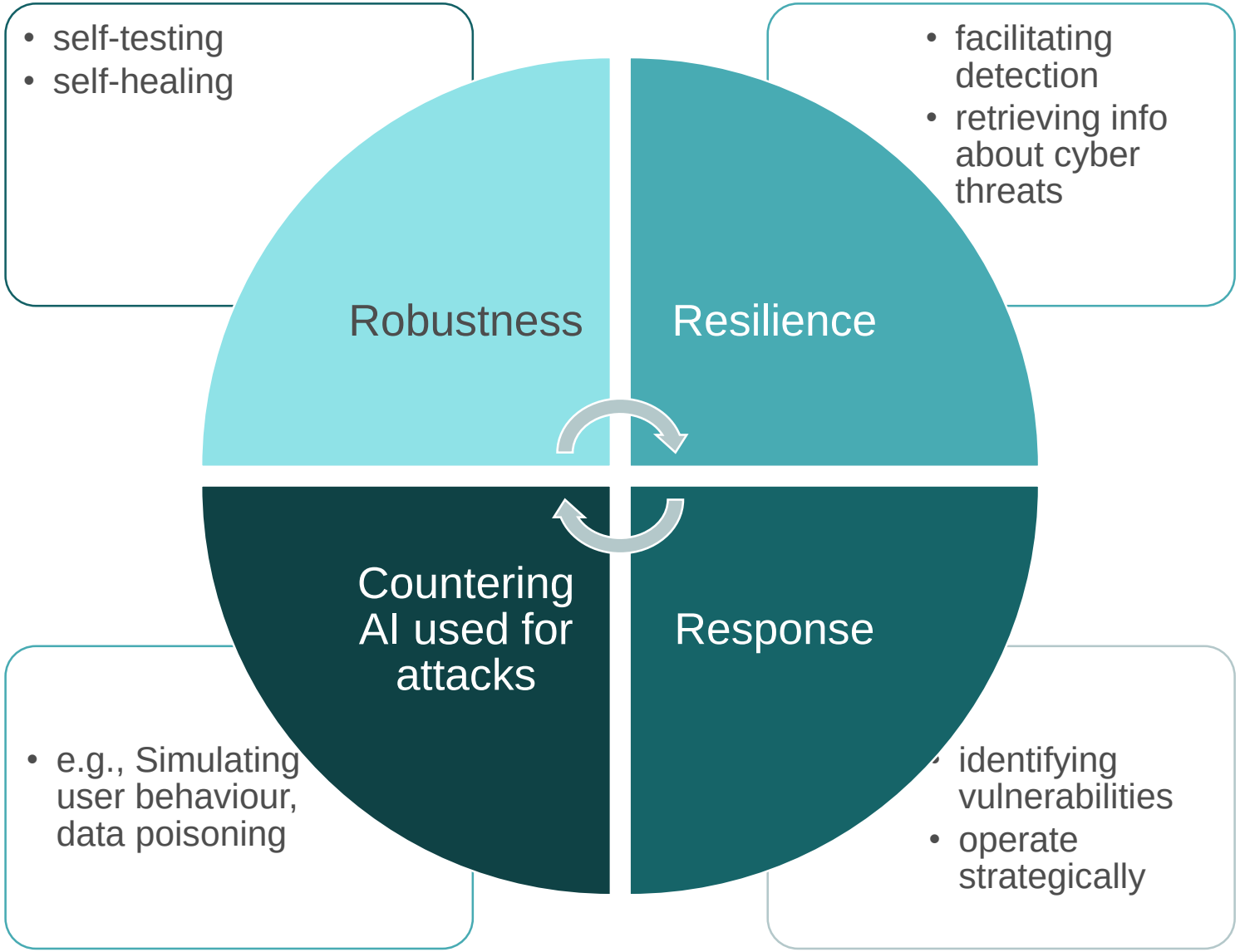
Expected Outcome

Projects are expected to contribute to some of the following expected outcomes:

- Reinforced cybersecurity using AI technological components and tools in line with relevant EU policy, legal and ethical requirements.
- Increased knowledge about how an attacker might use AI technology in order to attack IT systems.
- Digital processes, products and systems resilient against AI-powered cyberattacks

HORIZON-CL3-2021-CS-01-03: AI for cybersecurity reinforcement (2/3)

Scope



European Commission

HORIZON-CL3-2021-CS-01-03: AI for cybersecurity reinforcement (3/3)

- Expected EU contribution per project: EUR 3M – 4M
- Indicative topic budget: EUR 11M
- Type of Action: RIA (Research & Innovation Action)
- Technology Readiness Level: TRL4 (by the end of the project)

- Link to Participant Portal:

https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2021-cs-01-03

European Commission

HORIZON-CL3-2021-CS-01-04: Scalable privacy-preserving technologies for cross-border federated computation in Europe involving personal data

European Commission

HORIZON-CL3-2021-CS-01-04: Scalable privacy-preserving technologies for cross-border federated computation in Europe involving personal data (1/3)

Expected Outcome

Projects are expected to contribute to some of the expected outcomes:

- Improved scalable and reliable privacy-preserving technologies **for federated processing of personal data** and their **integration in real-world systems**.
- More **user-friendly solutions** for privacy-preserving processing of federated personal data registries by **researchers**.
- Improving privacy-preserving technologies for **cyber threat intelligence and data sharing** solutions.
- **Promotion of GDPR compliant European data spaces** for digital services and research.
- Strengthened **European ecosystem of open source** developers and researchers of privacy-preserving solutions.

HORIZON-CL3-2021-CS-01-04: Scalable privacy-preserving technologies for cross-border federated computation in Europe involving personal data (2/3)

Scope

- Address scalability and reliability of privacy-preserving technologies.

- Further research to ensure the applicability of the privacy-preserving computation. technologies in real-world use case scenarios.

- Integration with existing infrastructures and traditional security measures (e.g. access control).

- Respond to users' needs, e.g., in own personal data management for citizens or in personalised medicine.

- Address variations in legacy personal data models across different organisations.

- Include validation and/or piloting of in federated data infrastructures (European data spaces e.g. the EU heath data space).

- Be guided by EU's fundamental rights.

- Ensure *by-design* compliance with the GDPR.

- Interdisciplinary expertise, incl. legal expertise.

- Covering the supply and the demand side (i.e. industry, service providers and end-user).

- SMEs participation encouraged.

HORIZON-CL3-2021-CS-01-04: Scalable privacy-preserving technologies for cross-border federated computation in Europe involving personal data (3/3)

- Expected EU contribution per project: EUR 3M – 5M
- Indicative topic budget: EUR 17M
- Type of Action: RIA (Research and Innovation Action)
- Technology Readiness Level: TRL4 (by the end of the project)

- Link to Participant Portal:

https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2021-cs-01-04

General & Specific Conditions

- All topics cover RIA actions (100% funding)
- Admissibility, eligibility, financial and operational capacity and award criterial according the conditions set in the General Annexes. **Exceptions** regarding the use/production of **classified and sensitive information** apply. (See General Annex B)
- TRL #4 achievement expected by project completion under all topics
- The participation of SMEs is encouraged or strongly encouraged in all topics
- Integration of the gender dimension (sex and gender analysis) in research and innovation content is mandatory **except** in topic HORIZON-CL3-2021-CS-01-02 (hardware & supply chain)