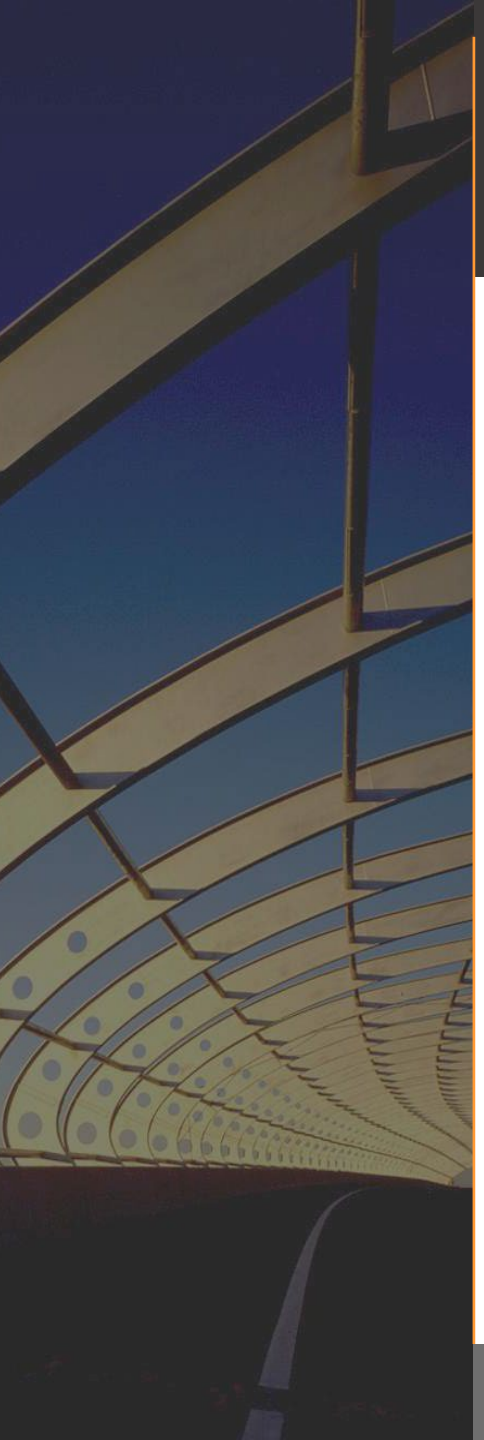
INNOVATION PROCUREMENT: CYBERSECURITY & DUAL USE

WORKSHOP-WEBINAR

13 January 2022

Watch the replay video of the webinar via: https://youtu.be/sFVeQ_L_r8c



Welcome

Stephan Corvers
CEO & Founder
Corvers Procurement Services BV

Introduction & Agenda

House rules

It is possible to ask questions in the private chat

The recording of the webinar will be made available on the EAFIP website

The list of participants will not be disseminated

In case there are technical problems, the session will be recorded and published

PART I

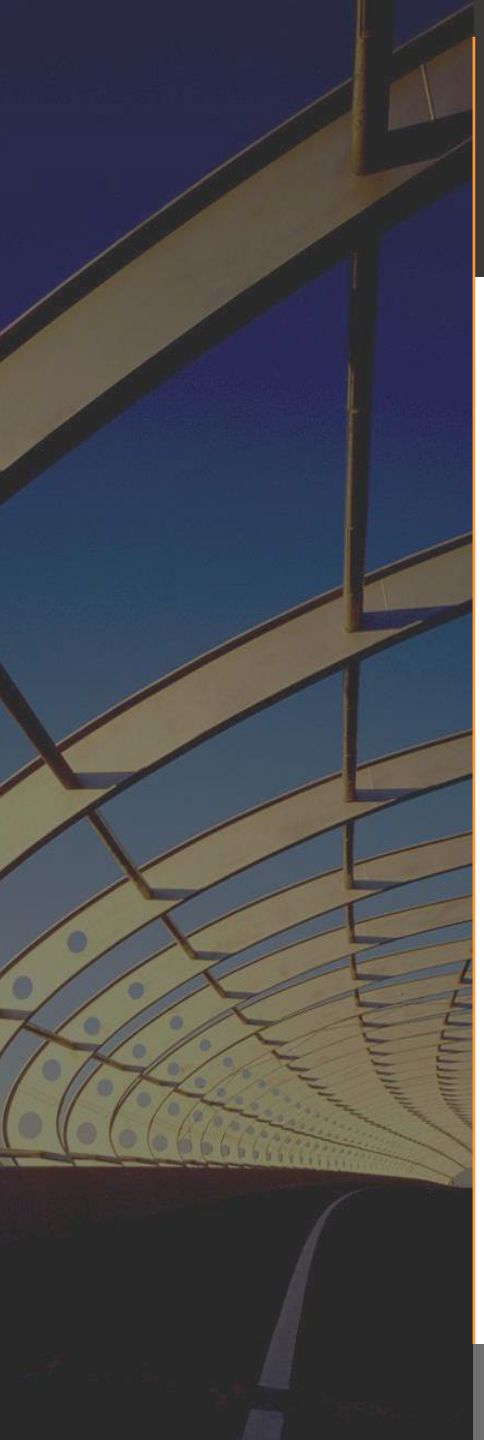
TIME (CET)	TOPIC	SPEAKER/PARTICIPANTS
09:25 – 09:30	Registration to the platform	Participants can ensure that the platform's functionalities are working fine
09:30 – 09:45	Welcome & Introduction House rules Agenda	Stephan Corvers CEO – Corvers Lieve Bos EC Policy Officer - DG Connect
09:45 – 10:05	CERIS Public procurement as a strategic catalyst of innovation in the security domain	David Rios Morentin Policy & Project Officer European Commission, DG HOME
10:05 – 10:25	EC initiatives on Cybersecurity	Aristotelis Tzafalias DG Connect – Cybersecurity Unity
10:25 – 10:45	**Q&A**	
10:45 – 11:00	**COFFEE BREAK**	

PART II

10:45 – 11:00	**COFFEE BREAK**	
11:00 – 11:25	PREVENT Joint cross-border Procurements of Innovative, Advanced Systems to Support Security in Public Transport (PCP)	Youssef Bouali Project Manager Engineering Ingegneria Informatica Spa, Italy
11:25 – 11:50	iProcureNet Joint Cross-Border Public Procurement and PCP	Jozef Kubinec Head of Works and ICT Procurement Department Ministry of Interior, Slovak Republic
11:50 – 11:55	**Q&A**	
11:55 – 12:00	**COFFEE BREAK**	

PART III

11:55 – 12:00	**COFFEE BREAK**	
12:00 – 12:25	Cyberagentur Human Brain Computer Interface (PCP)	Simon Vogt Vicepresident of Cyberagentur, Germany
12:25 – 12:50	Cyber Innovation Hub Dual use technologies launching customer (PPI)	Kor Gerritsma & Gertie Arts CIH, Ministry of Defence, The Netherlands
12:50 – 13:15	Public Procurement of Innovation and the National Cybersecurity Strategy: a Leverage Action for boosting Private Sector	Félix Barrio Juárez Deputy Director for the Cybersecurity of Citizens National Cybersecurity Institute, Spain
13:15 – 13:25	**Q&A**	
13:25 – 13:30	**Conclusions & future events**	**Stephan Corvers**



PART I

CERIS
Public procurement as a strategic catalyst of innovation in the security domain

David Rios Morentin
Policy & Project Officer
DG HOME, European Commission

Public procurement as a strategic catalyst of innovation in the security domain

EAFIP WORKSHOP-WEBINAR #3

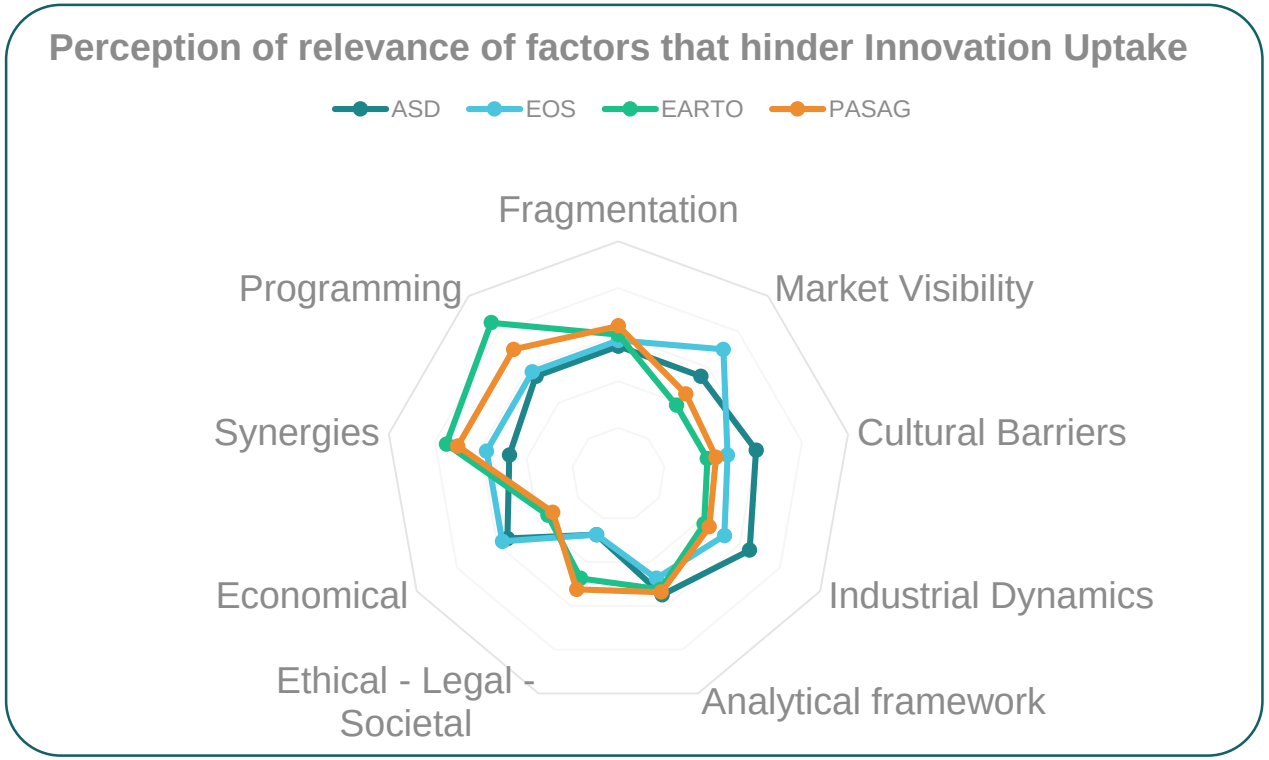
INNOVATION PROCUREMENT: CYBERSECURITY & DUAL USE

13 January 2022

David RIOS MORENTIN
SSRI Area Coordinator
Innovation and Security Research
European Commission – DG HOME

A more impactful Security R&I investment

- **EU investment for the development of capabilities in support to Policy priorities**
  - Innovation can be decisive: modernisation / effectiveness / efficiency
  - Uptake of innovation remains a challenge



* Based on internal analysis of latest position papers of EOS, ASD, EARTO and PASAG

European Commission

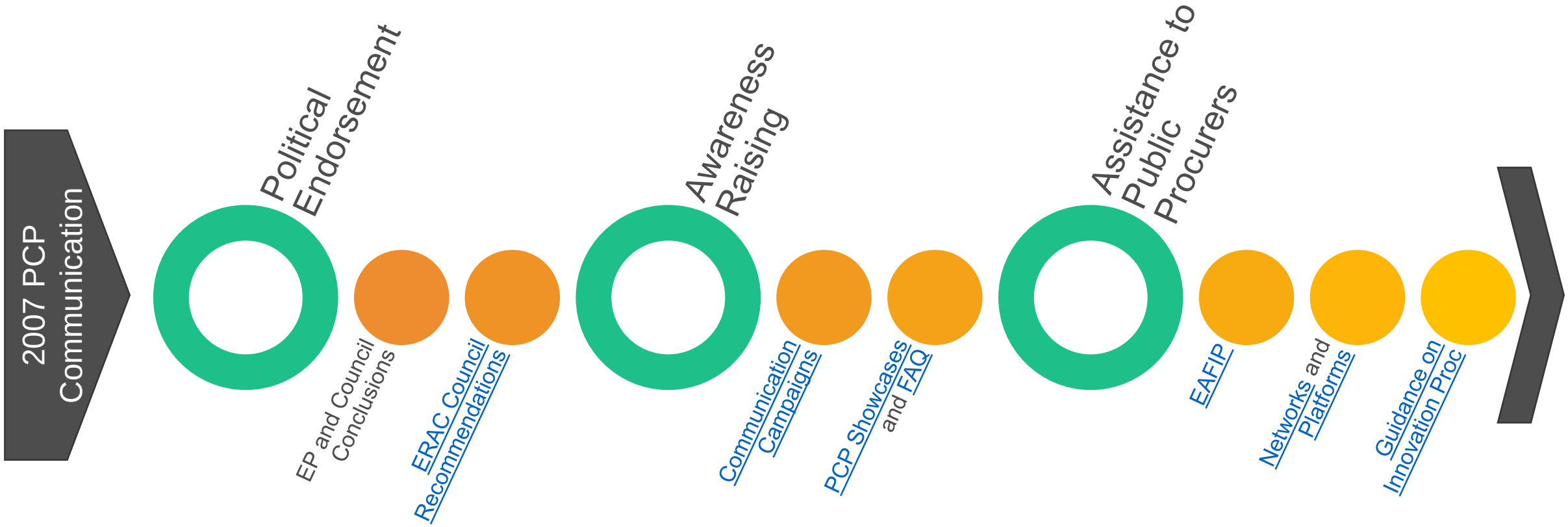
Road to Innovation Uptake

PROCUREMENT

- R&I is integrated in a wider **Capability Development Cycle** and its outcomes are considered as options.
- **Research needs** are defined non-prescriptively, on the basis of real threats, capability needs and gaps.
- **Resources** are made available for developers to undertake the necessary **research activities**
- Research is carried out under the **highest standards of excellence, impact and implementation**
- The **End-users** of security technologies are duly informed and take an active and substantial part in the research cycle
- Research results are **validated and endorsed** by the wider user community
- **Resources** are made available for **business creation, industrialisation and/or production scale-up**
- **Resources** are made available for the **acquisition** of innovative security solutions
- Users and buyers of security technology are aware of the **state of the art** and of how it matches with their needs
- The newly acquired innovative solutions are **deployed in the field of operations**

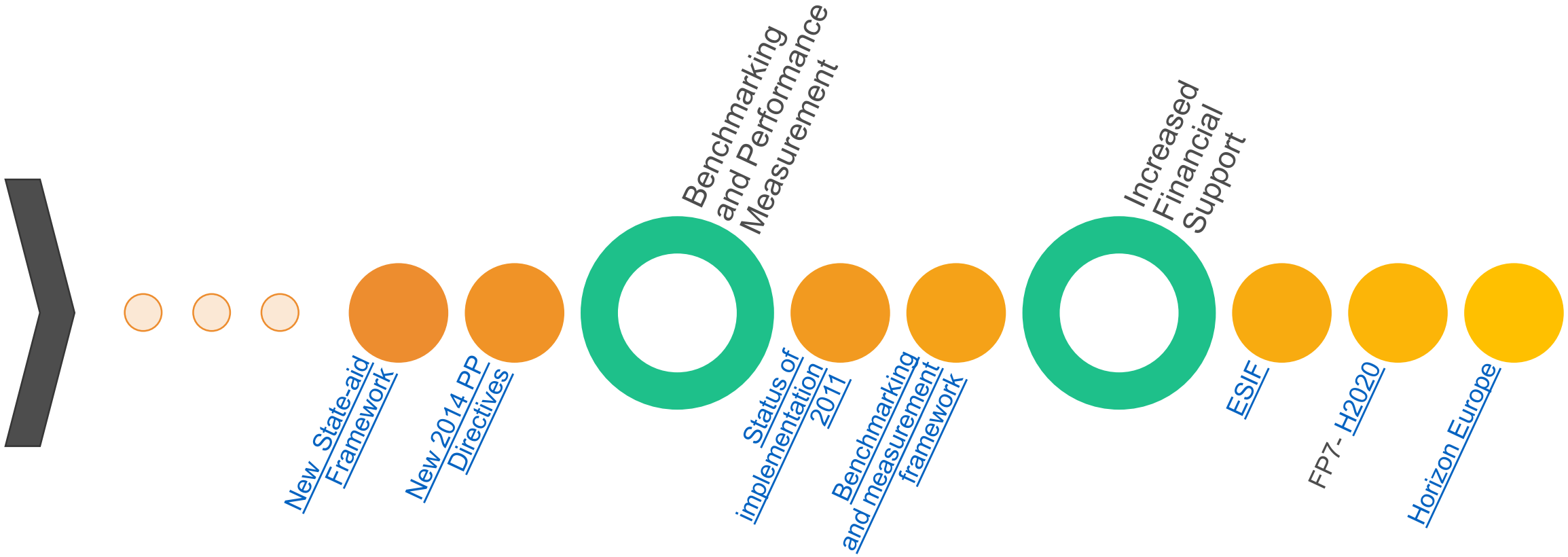
European Commission

Growing impact at European level



European Commission

Growing impact at European level



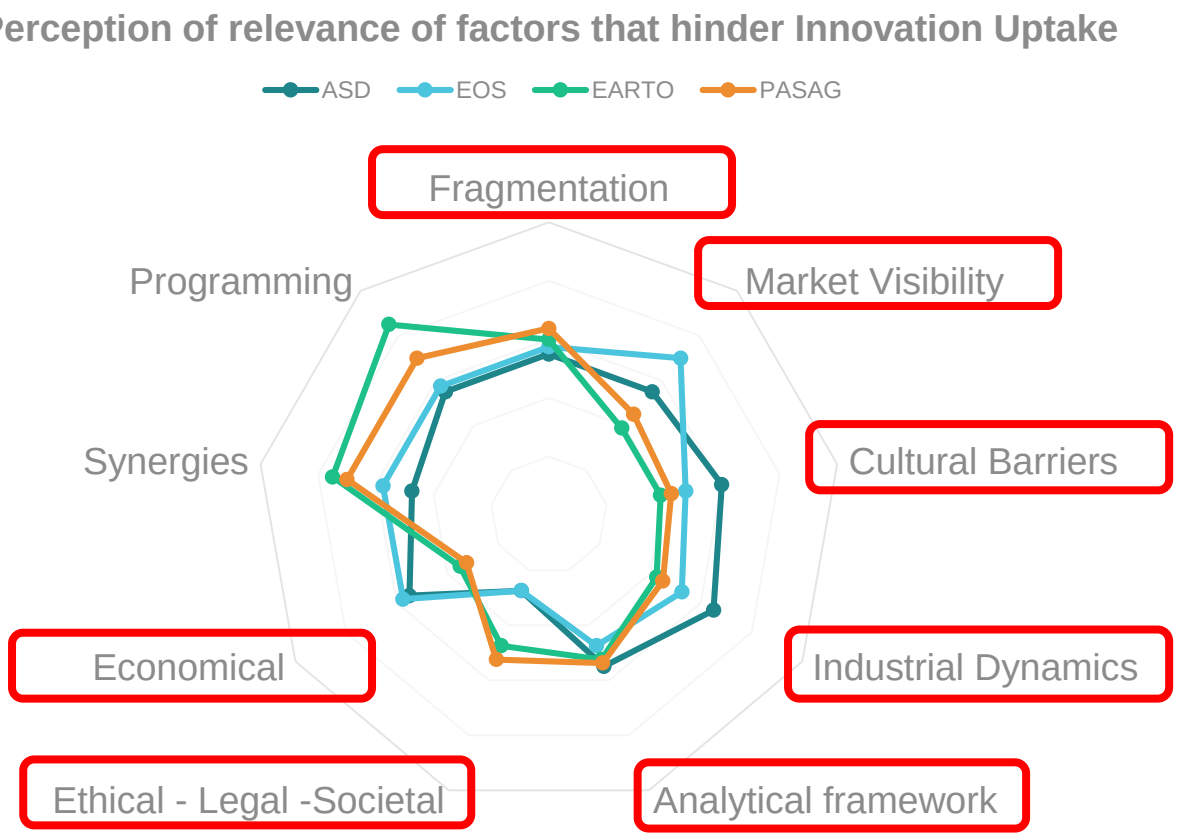
European Commission

EU-funded Security PCP projects

European Commission

What do we know so far?

- PCP projects contribute to overcoming barriers to innovation uptake in civil security



* Based on internal analysis of latest position papers of EOS, ASD, EARTO and PASAG

Assessment of EU-funded PCP projects

- Assessment report available online
- 5 PCP projects under study: CLOSEYE, EWISA, EUCISE2020, BROADWAY, SHUTTLE
- Assessment inspired on Commission notice Guidance on Innovation Procurement 2018
  - **Attracting innovators**
    - to measure how the tender for R&D services launched by the projects opened the door to small innovators, in particular high-tech start-ups and innovative SME's
  - **Attracting innovation**
    - to measure how the buyers attracted innovation within the procurement procedure by using innovation friendly tools and procedures

Assessment of EU-funded PCP projects

INNOVATORS

- Bureaucratic burden for tenderers
- Selection criteria
- Division into lots
- Use of standards, open data, open interfaces and open source software
- Payment schemes for main contractors
- Payment schemes for subcontractors
- Mobilisation of innovation brokers

INNOVATION

- How was the need expressed?
- How were the possible solutions to the problem explored?
- How were the tender requirements expressed?
- Did the tender allow variants?
- What was the award criteria?
- How were IPR managed?
- How was contract performance managed?

TENDER RESULTS

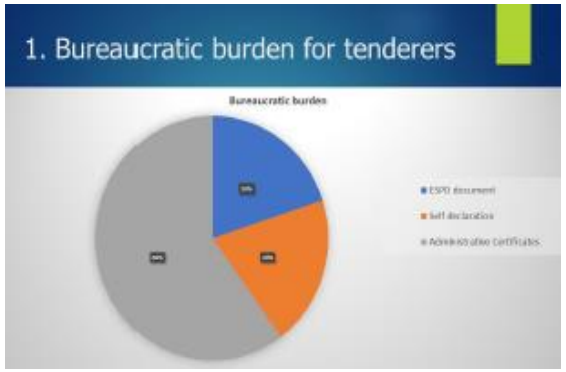
- SMEs acting alone or as lead bidder
- SMEs in consortia with large companies
- SMEs as subcontractors
- Bidders that are not from the country of the lead procurer
- Bidders that are not from a country of any project partner
- Subcontractors that are not from the country of the lead procurer
- Subcontractors that are not from a country of any project partner

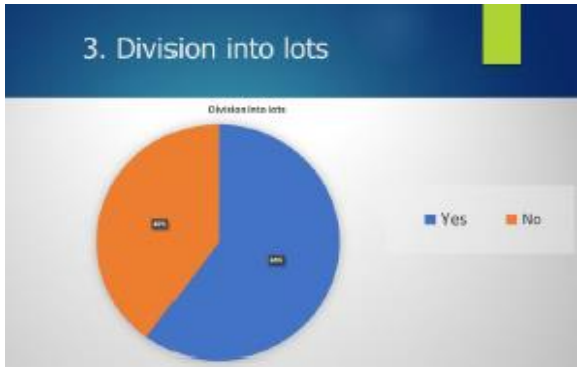
OBSTACLES

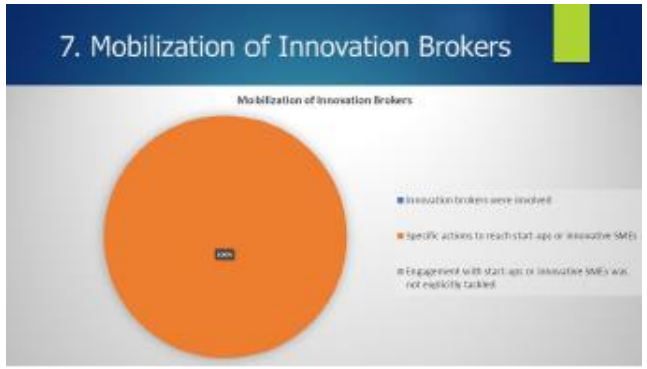
- Obstacles and hurdles for the implementation of the project

Blue : Best option
Orange : Second best option
Grey : Least good option

Assessment of EU-funded PCP projects





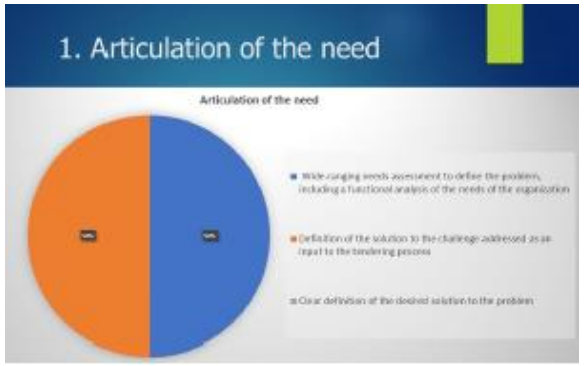


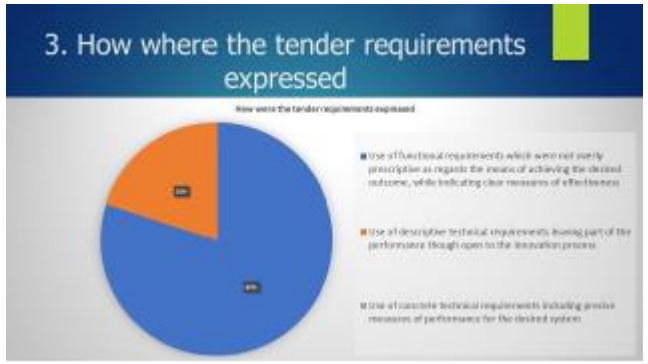
Procurement Approach - Innovators

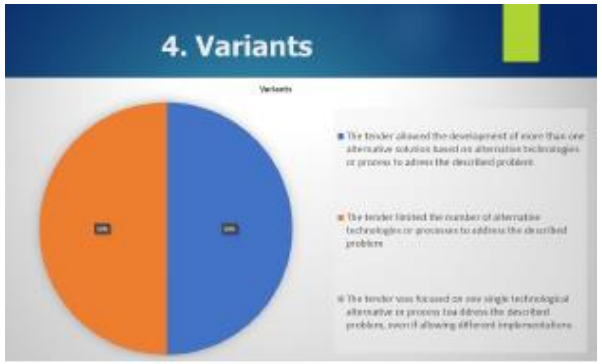
European Commission

Blue : Best option
Orange : Second best option
Grey : Least good option

Assessment of EU-funded PCP projects



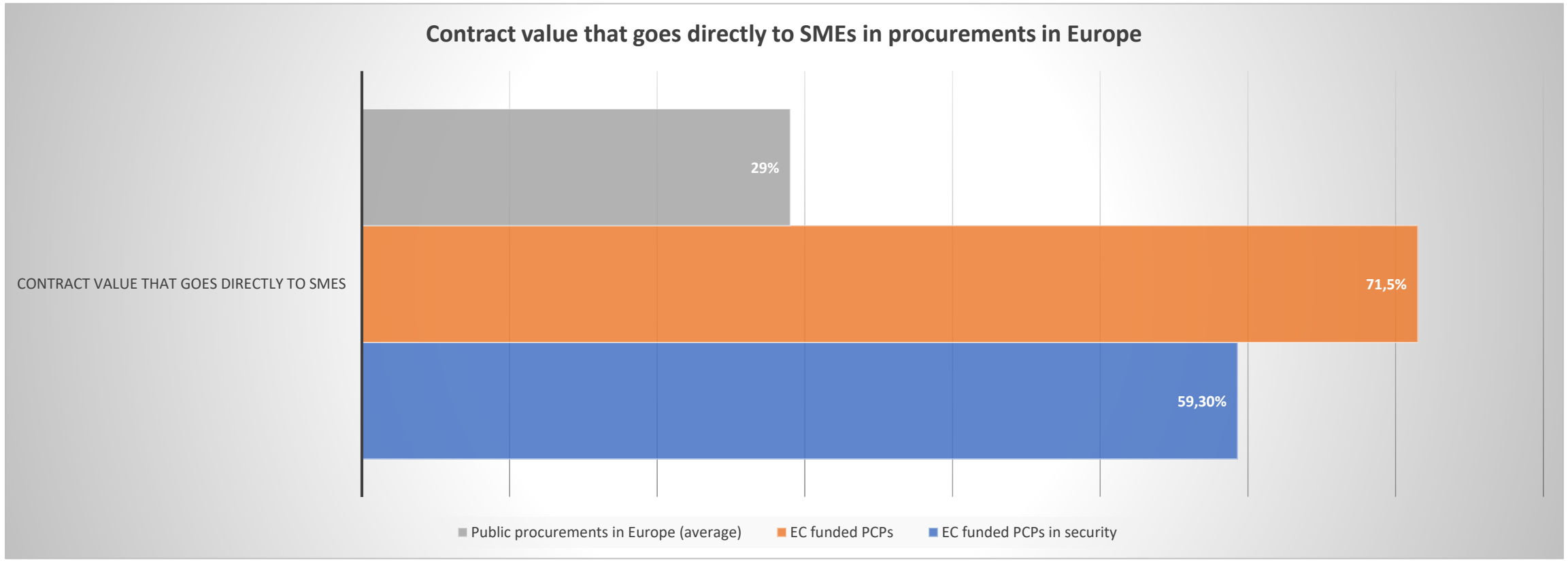




Procurement Approach - Innovation

European Commission

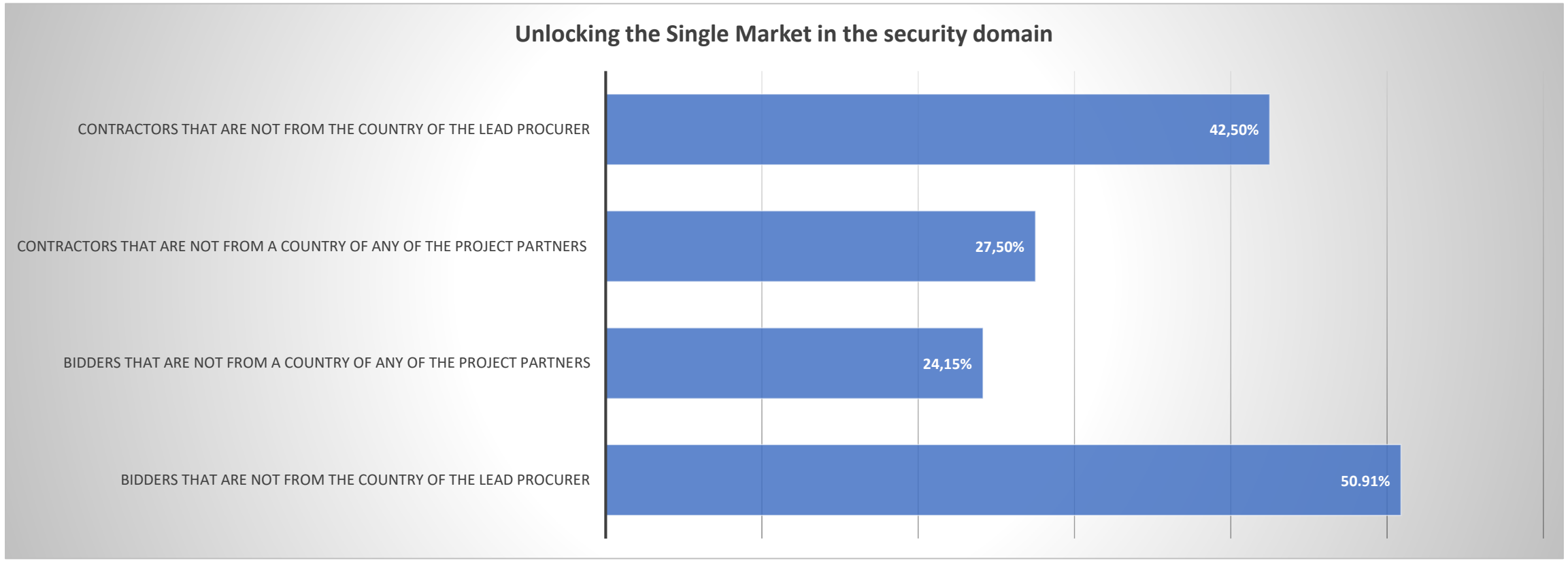
Assessment of EU-funded PCP projects



*"These projects have an impact in the EU public security market and economy, especially in terms of **enabling access to smaller innovators** (such as SMEs)…"*

European Commission

Assessment of EU-funded PCP projects



"… and of contributing to the **unlocking the European Single Market** in security."

European Commission

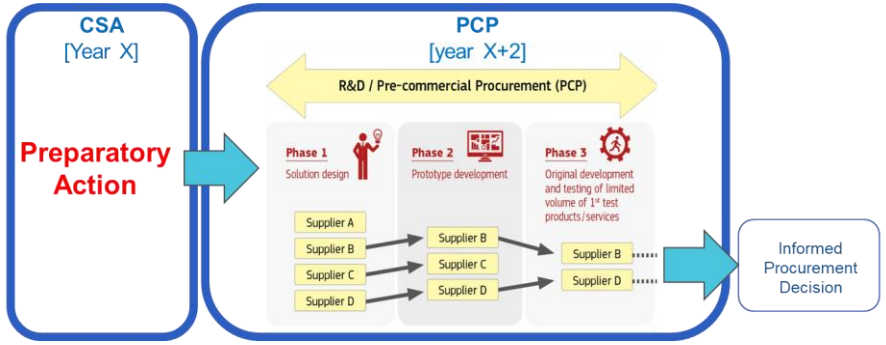
Way ahead at EU level

- Still few experiences in FP7 & H2020
  - Public procurers not yet aware of the opportunities;
  - The risk perceived is still high;
  - The capacity of public procurers to launch PCP/PPI needs to be further developed;
- There is margin for improvement at EU and Member State level:
  - Sustain an adequate level of funding for Innovation Procurement Actions;
  - Facilitate procurement process;
  - Awareness raising among public buyers and suppliers;
  - Foster the debate, increase the knowledge base and build a community;

European Commission

Sustain funding and facilitate process

- PCP in future calls
  - 2 steps process: CSA + PCP → Reduced risk and improved credibility by ensuring:
    - A structured demand
    - A variety of options to address the need exists
    - PCP tender is duly planned
    - Commitment to pursue the exploitation of results beyond the end of the project

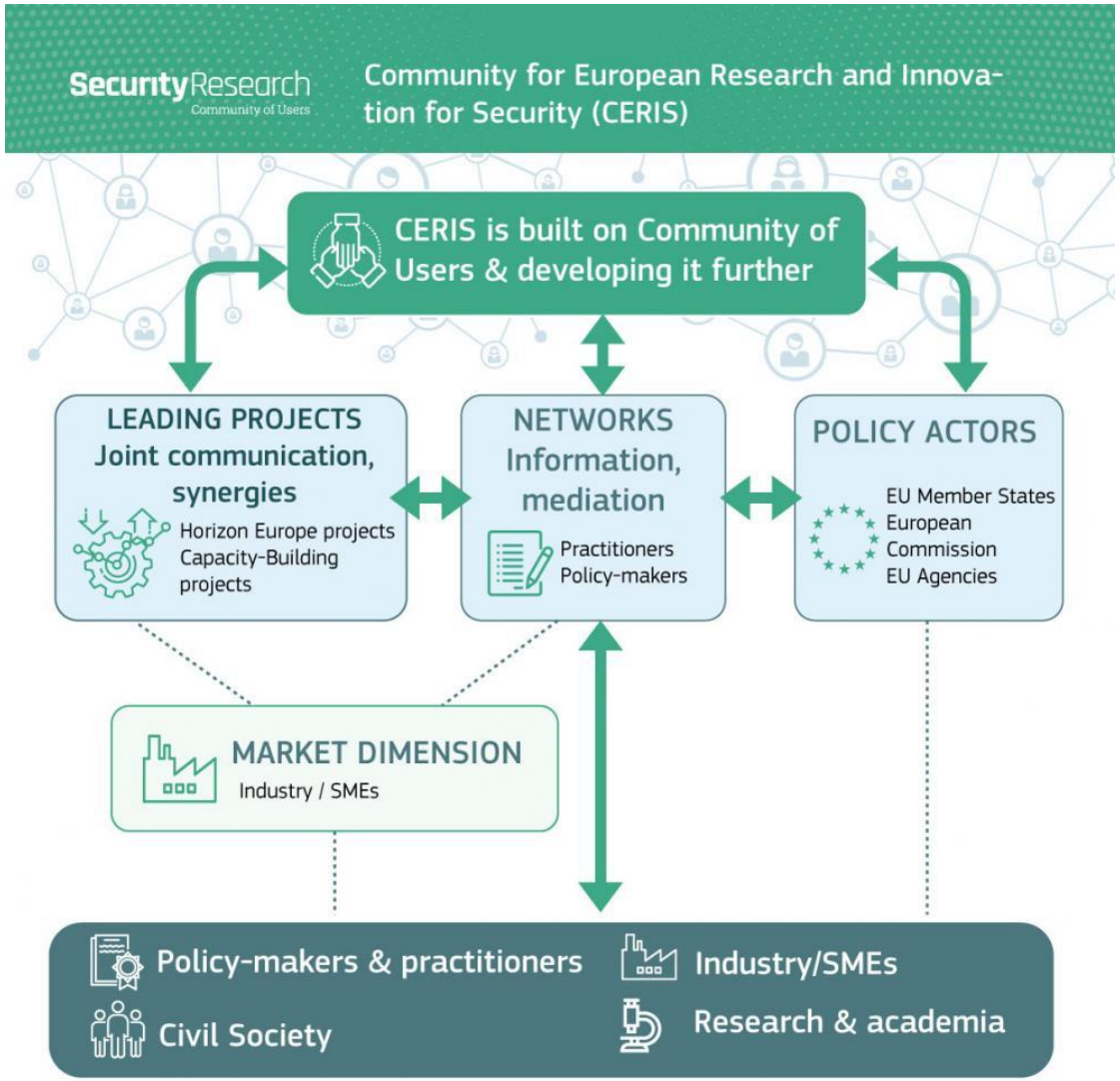


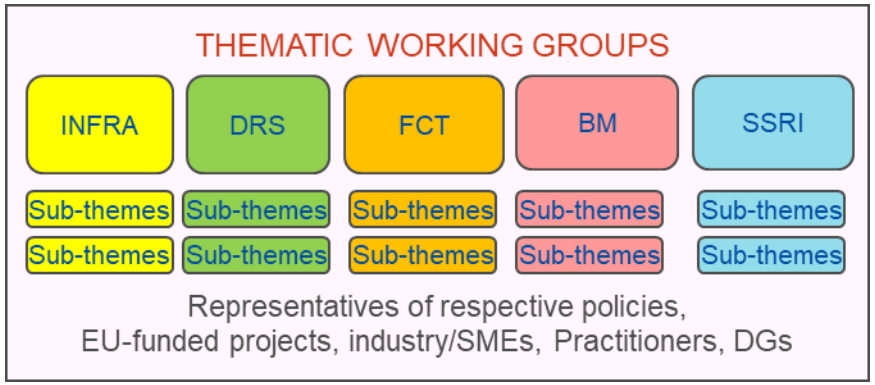
  - Clearer indications but not prescriptive – Bottom up PCPs (procurers need to get together, come up with ideas and show commitment)
  - General simplifications helping also less experienced procurers: Less red tape, more guidance on practical implementation issues (AGA, template tender docs), simpler reporting/payment

Rise awareness & identify opportunities

- Networks of practitioners
  - 14 Security Networks → The voice of the practitioners (What?)
    - Find common capability needs and, based on what is already available, the corresponding capability gaps;
    - Express common user/functional requirements for innovative solutions addressing the identified capability gaps;
    - Monitor state of the art technologies as well as research and innovation projects with a view to assessing the technological alternatives that match the requirements and recommending the uptake;
    - Indicate priorities as regards domains requiring more standardization.
  - iProcureNet → The voice of the procurers (How?)
    - Share investment plans;
    - Compare procurement techniques and rules;
    - plan for common procurements of research services as well as of innovative, off-the-shelf products

Knowledge creation and community building





- Community of European Research and Innovation for Security (CERIS)
  - **Thematic Workshops**
  - **interaction with existing networks**
  - **knowledge exchange & analytical tools**

European Commission

Knowledge creation and community building

- Three SSRI sub-areas

Industrial matters	Catalysts of uptake	Cross-cutting R&I
Characterisation of security market	Innovative Procurement	Foresight
SMEs and Start-ups	Stds. & Certification	Testing and Validation
Strategic autonomy (incl. FDI and other trade instruments)	Synergies between funds (V/H)	Technology assessment frameworks
Valorisation of IP		ELSE dimension
Business creation		Cross-cutting tech. R&I (e.g. Data, interoperability, AI, etc.)
Buyer-supplier relationship		

European Commission

CERIS - SSRI

https://ec.europa.eu/home-affairs/secure-safe-resilient-societies/index_en

European Commission

Search

CERIS - Community for European Research and Innovation for Security

Home | About | Thematic areas | Projects and Results | Events | Publications | Stay tuned

European Commission › CERIS - Community for European Research and Innovation for Security › Home

CERIS

Community for European Research and Innovation for Security

THEMATIC AREAS

1. BORDER MANAGEMENT (BM)
2. DISASTER RESILIENT SOCIETIES (DRS)
3. FIGHTING CRIME AND TERRORISM (FCT), INCL. INFRASTRUCTURE PROTECTION
4. STRENGTHENED SECURITY RESEARCH AND INNOVATION (SSRI)

4. STRENGTHENED SECURITY RESEARCH AND INNOVATION (SSRI)

EU R&I funding has contributed substantially to knowledge and value creation in the field of civil security and to the consolidation of an ecosystem better equipped to capitalise on research and innovation to support the EU's security priorities. However, a key challenge remains in improving the uptake of innovation.

There are factors that limit the impact of EU security R&I by hindering the uptake of its outcomes. They include market fragmentation, cultural barriers, analytical weaknesses, ethical, legal and societal considerations and a lack of synergies between funding instruments, among others. Such factors equally affect the various security domains and complex relationships between them are difficult to disentangle.

The aim of the Strengthened Security Research and Innovation (SSRI) area is to create a favourable environment to generate the knowledge required to tackle the abovementioned factors.

The CERIS SSRI working group will be the designated platform to foster a more structured dialogue between all relevant market actors. It will allow for the exchange of knowledge to enable increased innovation uptake that reverberates on a more competitive and resilient EU security technology and industrial base, hence contributing

Events (6)

RSS

Showing results 1 to 6

STATUS: Past ⊗ | Upcoming and ongoing ⊗

KEYWORDS: SSRI ⊗

18 OCT 2021 — CONFERENCES AND SUMMITS
SSRI Workshop #5: Evaluation of innovative security technologies: Building credibility as a step towards uptake

05 JUL 2021 — INFO DAYS
CERIS – SSRI – EU Security Market Study

02 JUL 2021 — TRAINING AND WORKSHOPS
CERIS SSRI virtual workshop Public Procurement as a catalyst of innovation for security

28 JUN 2021 — PARTNER MEETINGS | RESCHEDULED
CERIS – SSRI - National / Regional Community Building - Experiences and perspectives

04 JUN 2021 — TRAINING AND WORKSHOPS
CERIS-SSRI virtual workshop: Uptake stories: 3 avenues from R&I to deployment

30 APR 2021 — CONFERENCES AND SUMMITS
Challenges and opportunities for SMEs and start-ups in EU security R&I

What we like about Innovation Procurement

Suppliers

- **Access to new/small players**
- Shorter Time to market
- Faster company growth
- Economies of scale
- Wider market / cross-border

Policy makers

- Implement political priorities
- **Modernize public services**
- Improve innovation ecosystem
- Attract foreign investment
- Create growth and jobs

- New lead markets
- Increase export
- Global **competitiveness**

-First customers

-**Shared risks & benefits**

Win-win for all !!

- **Cheaper / better products**
- Lower risk of modernization

Procurers

- **Shape product development to public needs**
- Increase technology knowledge
- Reduce risk in commercial tendering
- **Reduce supplier lock-in** and open up market to smaller players

Get the 'Best Product'…

- **Economies of scale**
- Usage / Licensing rights
- 'First time right' product
- **'EU interoperable'**
- Attractive to venture capitalists
- Reduce unforeseen expenditure

… at the 'Lowest Price'

European Commission

Thank you

#HorizonEU

#EUsecurityResearch

CERIS Website

EU Funding and Tenders Portal

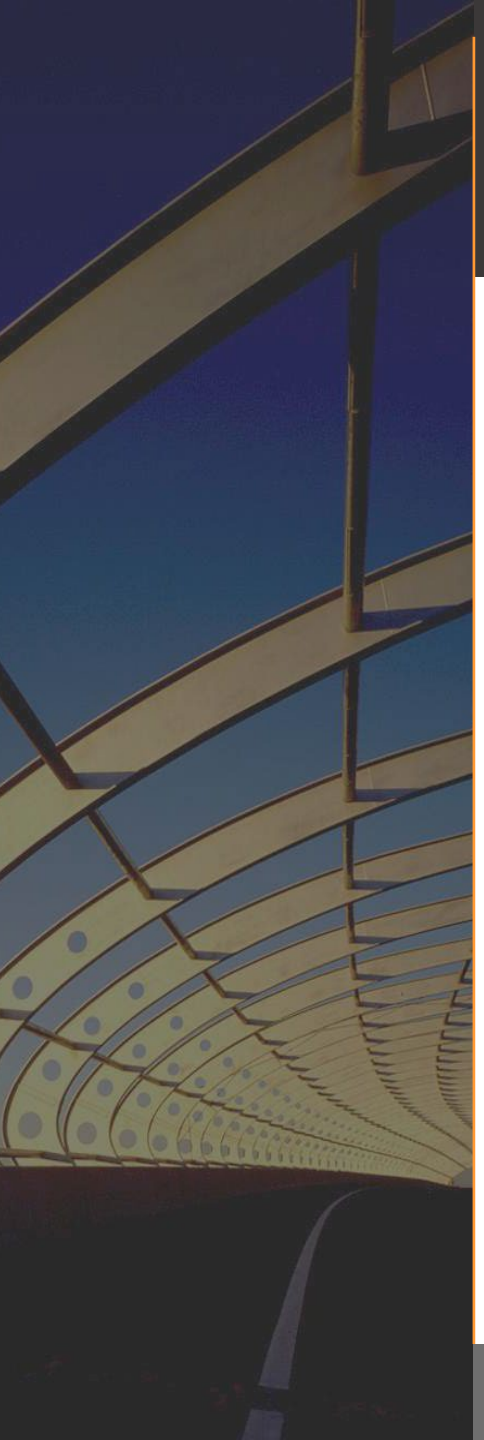
EU Innovation and Industry for Security

Horizon Europe Cluster 3 "Civil Security for Society"

David RIOS MORENTIN
SSRI Area Coordinator
Innovation and Security Research
European Commission – DG HOME

http://www.linkedin.com/in/driosmorentin

European Commission



EC initiatives on Cybersecurity

Aristotelis Tzafalias
DG Connect – Cybersecurity Unity

European Union initiatives in Cybersecurity – Public Administration in the NIS 2.0

European Assistance for Innovation Procurement (EAFIP)

WEBINAR Workshop – Innovation Procurement : Cybersecurity & dual use

1

NIS 2.0 OVERVIEW

European Commission

Main challenges of existing NIS 1

Not all sectors that may be considered critical are in scope

Great inconsistencies and gaps due to the NIS scope being *de facto* defined by MS (case by case OES identification)

Diverging security requirements across MS

Diverging incident notification requirements

Ineffective supervision and limited enforcement

Voluntary and ad-hoc cooperation and info sharing between MS and between operators

The NIS 2 vision - main objectives

1

Cover a larger portion of economy and society (**more sectors, including public administration**)

2

Within sectors: systematically focus on bigger and critical players (**replace current identification process**)

3

Align security requirements (incentivize investments and awareness including by mandating board-level accountability), expand **supply chain** and supplier relationships risk management

4

Streamline incident reporting obligations

5

Align provisions on national supervision and enforcement

6

More operational cooperation approach including on crisis management

7

Align with proposed Resilience of Critical Entities Directive

European Commission

Three main pillars of the proposal for NIS 2

MEMBER STATE CAPABILITIES

National authorities

National strategies

CVD frameworks

Crisis management frameworks

RISK MANAGEMENT

Accountability for top management for non-compliance

Essential and important companies are required to take security measures

Companies are required to notify incidents

COOPERATION AND INFO EXCHANGE

Cooperation Group

CSIRTs network

CyCLONe

CVD and European vulnerability registry

Peer-reviews

Biennial ENISA cybersecurity report

2

MEMBER STATE CAPABILITIES

European Commission

National cybersecurity frameworks

- National cybersecurity strategies
  - Including “guidelines regarding the inclusion and specification of cybersecurity-related requirements for ICT products and service in public procurement”;
- National **Cybersecurity Crisis Management Frameworks**
- Framework for **Coordinated Vulnerability Disclosure**
- Competent authorities in charge of implementation
- Single Points of Contact (SPOCs) to liaise between Member States
- National Computer Incident Response Teams (CSIRTs)

European Commission

3

CYBERSECURITY RISK MANAGEMENT IN PUBLIC ADMINISTRATION

European Commission

Which sectors are covered?

Essential entities	Important entities
Energy (electricity*, district heating, oil, gas and hydrogen)	Postal and courier services
Transport (air, rail, water, road)	Waste management
Banking	Chemicals (manufacture, production, distribution)
Financial market infrastructures	Food (production, processing, distribution)
Health (healthcare, EU reference labs, research and manufacturing of pharmaceuticals and medical devices)	Manufacturing (medical devices; computer, electronic and optical products; electrical equipment; machinery; motor vehicles and (semi-)trailers; transport equipment)
Drinking water	Digital providers (search engines, online market places and social networks)
Waste water	
Digital Infrastructure (IXP, DNS, TLD, cloud, data centres, CDN, electronic communications and trust service providers)	
Public administration	
Space	

*** New types of entities in electricity:** electricity markets, production, aggregation, demand response and energy storage

European Commission

Cybersecurity requirements

- Accountability for top management for non-compliance with cybersecurity risk management measures
- Risk based approach: appropriate and proportionate technical and organisational measures
- Measures to at least include:

  - risk analysis and information system security policies
  - incident handling
  - business continuity and crisis management
  - supply chain security
  - security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure
  - policies and procedures to assess the effectiveness of cybersecurity risk management measures
  - policy on the use of cryptography and encryption

Emphasis on supply chain cybersecurity

- Supply chain security is **one of the security measures** that essential and important entities need to take into account
- Member States are required to address cybersecurity in the supply chain for ICT products and services for essential and important entities in their **national cybersecurity strategies**
- The **Cooperation Group** is explicitly empowered with carrying out coordinated security risk assessments of specific critical ICT services, systems or products supply chains (based on the example of 5G)

European Commission

4

EU COOPERATION, INFORMATION EXCHANGE AND CRISIS MANAGEMENT

European Commission

Cooperation and information sharing

- **Cooperation Group** gathering competent authorities
- **CSIRTs network** gathering national CSIRTs
- SPOCs to submit **monthly incident summary** reports to ENISA
- Framework of specific **cybersecurity information-sharing arrangements** between companies
- Voluntary information sharing
- **Peer-reviews** of the Member States' effectiveness of cybersecurity policies

European Commission

Crisis management

National Cybersecurity Crisis Management Frameworks

European Cyber Crises Liaison Organisation Network, EU – CyCLONe, is established to support the coordinated management of large-scale cybersecurity incidents and crises

Coordinated vulnerability disclosure

- As part of the national cybersecurity strategy, Member States will be required to develop a **policy framework on coordinated vulnerability disclosure**
- Each Member State shall be required to designate one **national CSIRT as a coordinator** and facilitator of the coordinated vulnerability disclosure process at national level.
- In cases where the reported vulnerability affects multiple vendors across the Union, the designated CSIRT shall cooperate with the CSIRT network to facilitate multi-vendor coordinated vulnerability disclosure.
- **European vulnerability registry** run by ENISA

European Commission

5

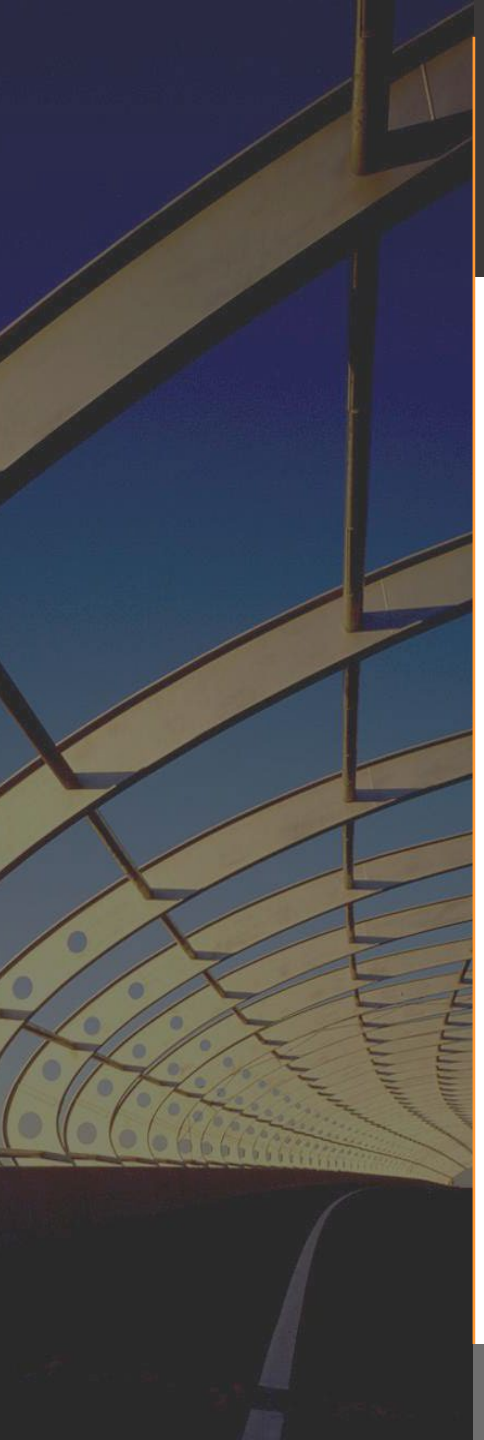
SUMMARY

European Commission

Summary

- Public administration ‘dual’ responsibility in NIS 2.0: increase overall cybersecurity in national economy and society but also improve cybersecurity of public services.
- NIS 2.0 expands the scope to **include public administration** as essential entities subject to cybersecurity risk management and incident reporting requirements.
- Increasing emphasis on cybersecurity in (public) procurement, security-by-design, full life-cycle, supply chain security.
- Evolving threat landscape and technological innovation drives the constant need for innovative products and services.

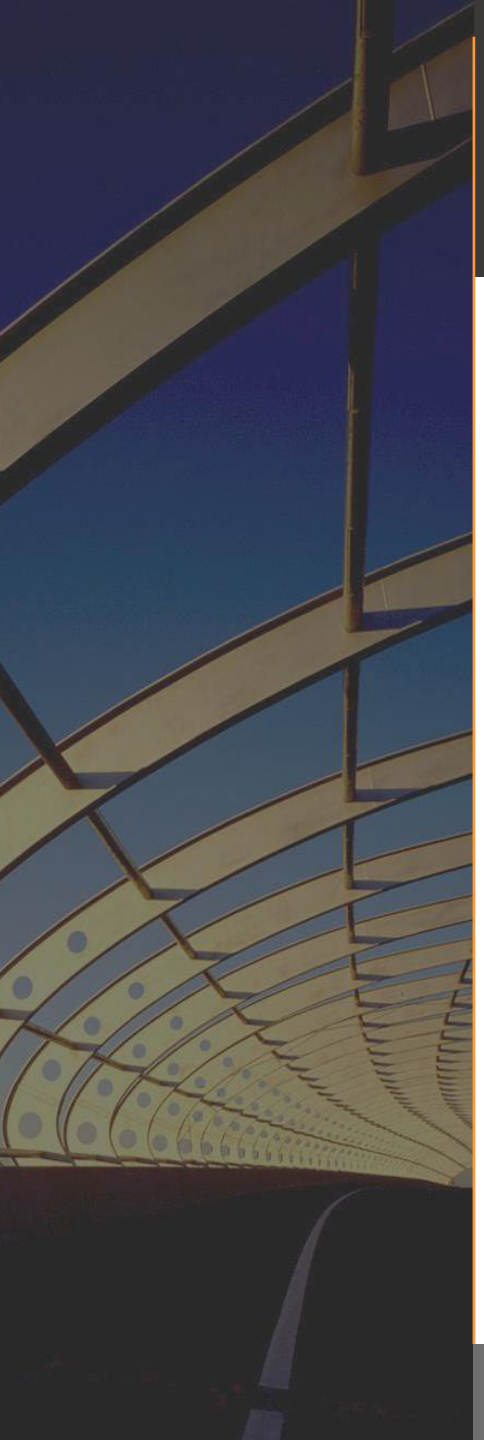
European Commission



Poll

Q&A


COFFEE BREAK



PART II

PREVENT
Joint cross-border Procurements of Innovative, Advanced Systems to Support Security in Public Transport (PCP)

Youssef Bouali
Project Manager
Engineering Ingegneria Informatica Spa, Italy

PRocurEments of innoVativE, advaNced systems to support security in public Transport – Pre-Commercial Procurment

Youssef Bouali, Engineering Ingeneria Informatica SpA

13th January 2022, EAFIP Workshop

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020374

Project details

Call: H2020-SU-SEC-2020

Topic: SU-GM02-2020 *Strategic pre-commercial procurements of innovative, advanced systems to support security*

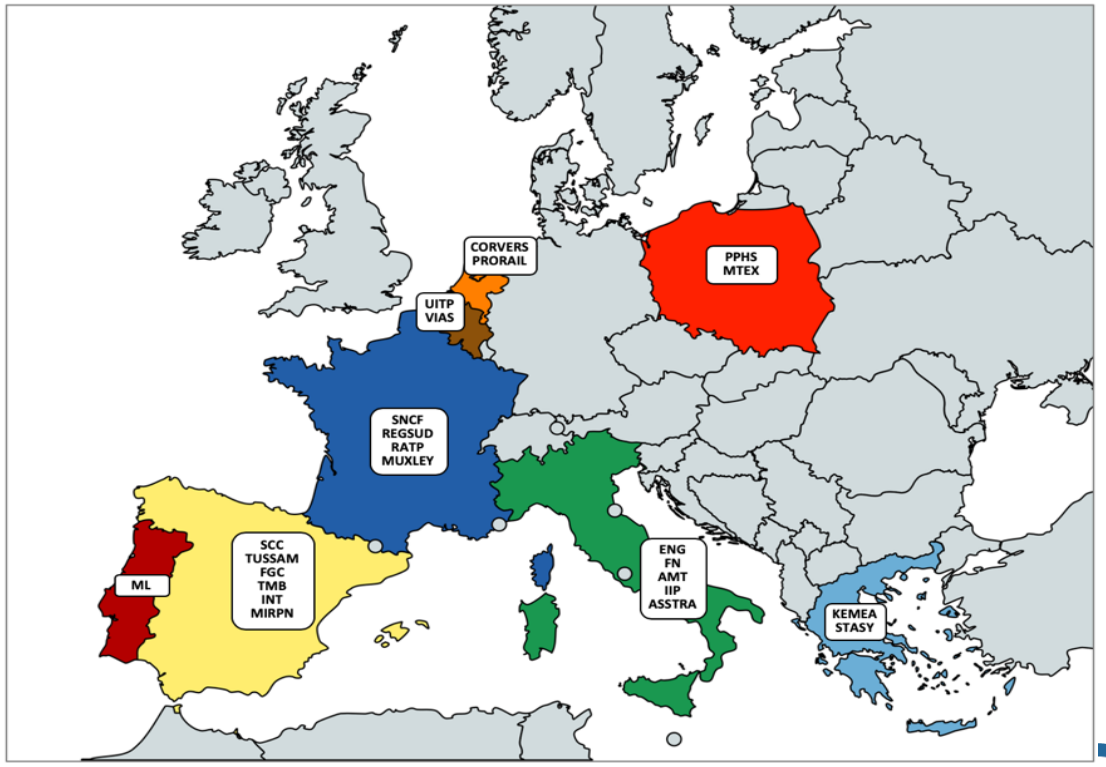
Start: 1 September 2021
End: 31 August 2024

Budget: €13,3 Million

Project coordinator:

Engineering Ingegneria Informatica S.p.A.
Youssef Bouali
youssef.bouali@eng.it

23 Partners
8 Countries
12 Public Buyers / 10 Transport Operators / 2 LEAs



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020374

Partners

ENGINEERING

Advisors

CORVERS
COMMERCIAL & LEGAL AFFAIRS

ISTITUTO ITALIANO PER LA PRIVACY E LA VALORIZZAZIONE DEI DATI

VAS institute

CoU

UITP ADVANCING PUBLIC TRANSPORT

ASSTRA

POLISH PLATFORM FOR HOMELAND SECURITY

Public Buyers & PTOs

KEMEA

RÉGION SUD PROVENCE ALPES CÔTE D'AZUR

NO8DO AYUNTAMIENTO DE SEVILLA

SNCF

Metropolitano de Lisboa

RATP GROUP

FERROVIENORD FNM GROUP

TUSSAM

AMTGenova

FGC Ferrocarrils de la Generalitat de Catalunya

ProRail

TMB Transports Metropolitans de Barcelona

Technical

MORATEX INSTYTUT

MUXLEY

LEAs

mossos d'esquadra

Goal

The global aim of PREVENT PCP is to

augment the security

in **public transport**

through **innovative procurement** of technology solutions.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020374

Goal

The project aims to deliver and equip Public Transport Operators with solutions enhancing security situational awareness through

Timely automatic detection of potentially dangerous unattended items in Public Transport Infrastructure and in public areas in the vicinity

Identification and tracking of perpetrators

Advanced crisis management system

The need for innovative solutions stems from a **longer collaboration** and is driven by **commonly identified internal needs** to improve the quality and efficiency of pre-empting terrorist attacks.

The PREVENT PCP project builds on the **outcomes of its predecessor PREVENT**, and it continues the top-down approach that allowed consolidating **commonly agreed scenarios**, covering the critical security issues down to a detailed identification of the **complete set of innovation needs**, both at process and technology levels, to ease coordination across the **full chain of stakeholders, from transport operators to security forces and public authorities**.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020374

PREVENT

PRocurEments of innoVativE, advaNced systems to support security in public Transport

- A COMMON ***SECURITY DIAGNOSTICS AND VULNERABILITY*** TAXONOMY
- A ***SCENARIOS ELABORATION*** METHODOLOGY
- A SET OF **6** ***USE CASES*** CONSOLIDATING THE KEY SECURITY CHALLENGES IN PUBLIC TRANSPORT, AND INTEGRATING THE GDPR AND ECONOMIC CAPABILITIES DIMENSIONS
- A ***ROADMAP OF INNOVATION NEEDS*** TO ADDRESS THESE KEY CHALLENGES, INTEGRATING THE GAPS WITH RESPECT TO AVAILABLE SOLUTIONS
- A FULLY DETAILED AND AGREED **COMMON CHALLENGE** FOCUSED ON THE HIGHEST PRIORITISED NEED FROM THE ROADMAP
- TO ***INITIATE A PCP***, SPEEDING UP ITS IMPLEMENTATION THROUGH A FOLLOW-UP ACTIVITY BEYOND THE END OF PREVENT

TOPIC: SU-GM02-2018 - STRATEGIC PRE-COMMERCIAL PROCUREMENTS OF INNOVATIVE, ADVANCED SYSTEMS TO SUPPORT SECURITY

GA N°: 833444

DURATION: 15 MONTHS

START DATE: 01/05/2019

END DATE: 31/07/2020

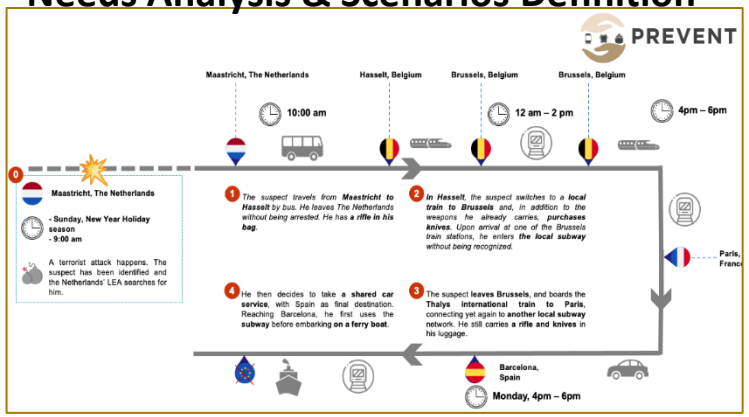
WEBSITE: HTTPS://PREVENT.ENG.IT

COORDINATOR: ENGINEERING INGEGNERIA INFORMATICA SPA

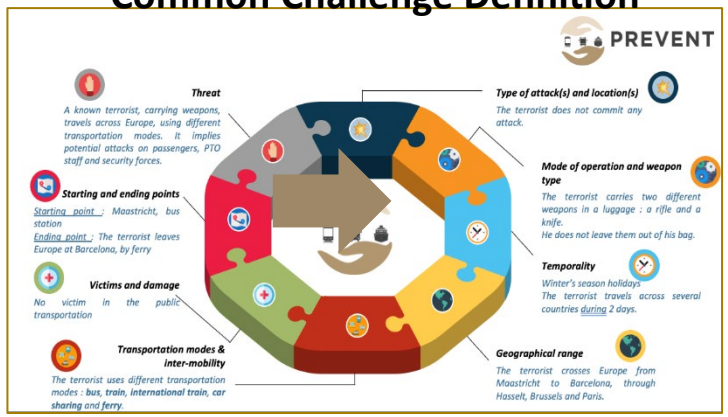
PREVENT

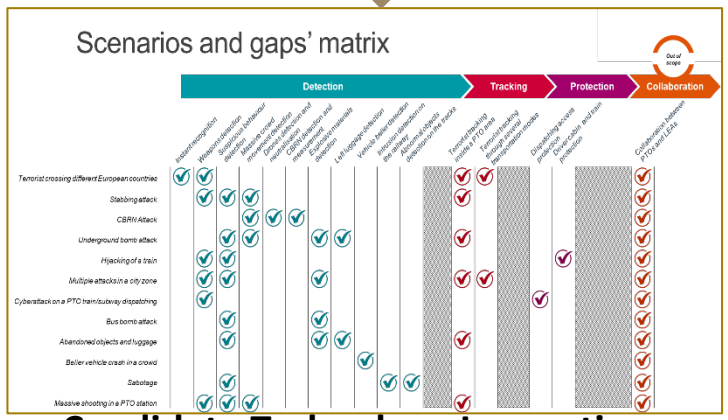
Major Milestones

Needs Analysis & Scenarios Definition

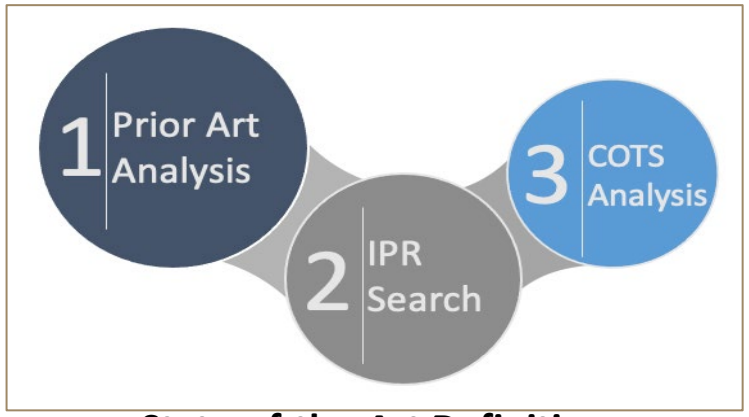


Common Challenge Definition





Candidate Technology Innovations



State-of-the-Art Definition

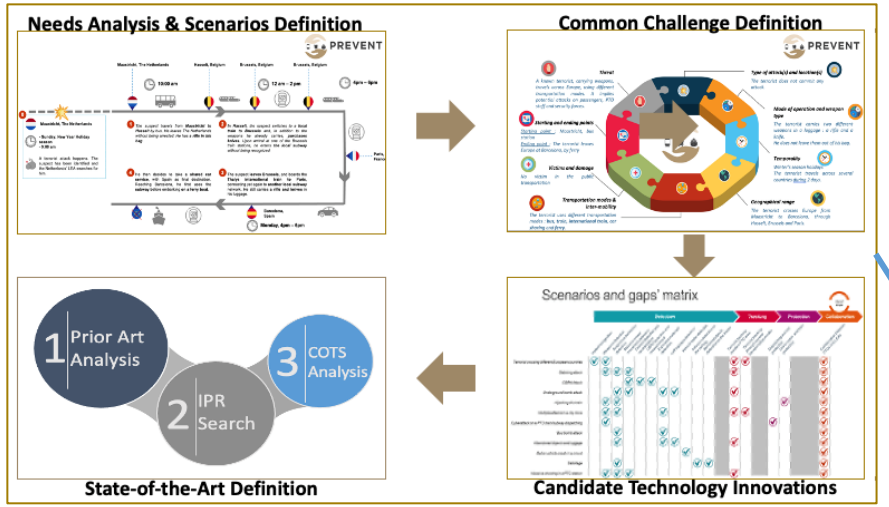
Identified needs are indeed **UNMET.**

→ Require R&D to bring the State- of-the-Art up to the point of commercialization

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020374

PREVENT

Major Milestones



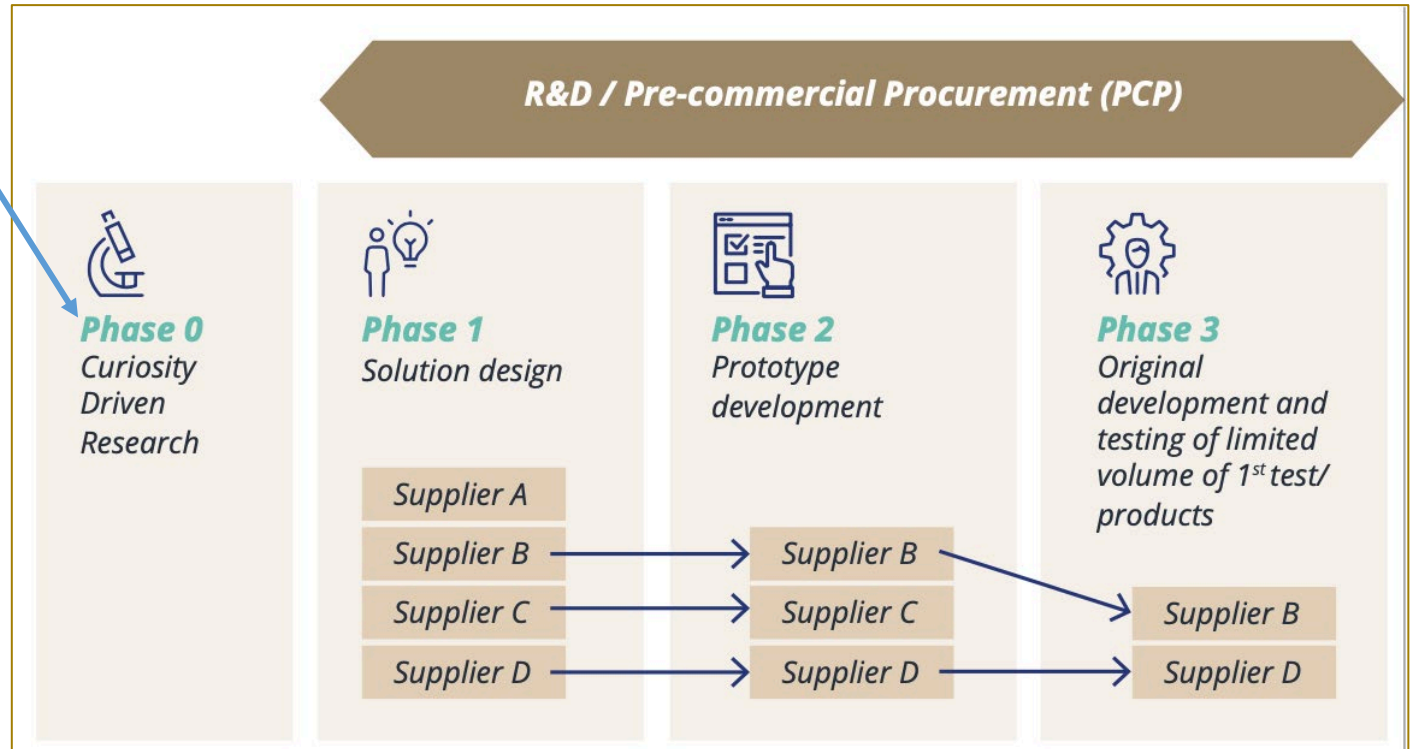


Figure 1. PCP and PPI process. Source: European Commission

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020374

Approach

PREVENT PCP is based on the results, common challenge and synergies resulting from PREVENT CSA

PREVENT PCP is a demand-side effort enabling the public buyers to engage with innovative businesses to develop and deliver novel solutions

It involves a risk-benefit sharing under market conditions: IPR ownership rights of the R&D in exchange of lower development prices

Procurement of R&D services organised in competitive phases - clear separation between the procurement of R&D services from the deployment of commercial volumes of end-products (PPI).

PREVENT PCP ensures the involvement of all the relevant stakeholders through the User Observatory Group

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020374

Involvement of Actors

1 - Buyers Group

The group of end users provides financial commitments in order to execute the PCP. Their objective is to obtain an innovative and cost-effective solution that will enhance the situational awareness in their premises: **KEMEA, REGSUD, SNCF, RATP, SCC, TUSSAM, FGC, TMB, ML, FN, AMT, PRORAIL, KTEL**

2 - LEAs

Represent the first responders organizations who will provide valuable input in the requirements formulation based on their experience as well as evaluating the project outcomes along with the Buyers Group members: **INT**, **MIRPN**, (**HP** and **Seville LP**)

3 - Lead procurer

KEMEA, Center for Security Studies which is the public procurer jointly appointed by the buyers' group to lead the PCP action. Its role is to be the legal entity that executes the procurement processes

4 - Technical Advisors

Consists of partners with technological expertise who will guide/ consult the buyers' group to set realistic, clear and ambitious specifications, objectives and requirements for the solution to be developed. The technical advisors are **ENG**, **MORATEX** and **MUXLEY**

5 - Legal Advisors

For the successful completion of the project two Legal Advisors' contribution is considered crucial in order to map the legal boundaries in terms of the GDPR compliance and the PCP activities. In this regard, **IIP** and **CORVERS** will contribute to that direction

6 - Social Advisor

VIAS will cover the societal aspects including the acceptance of the solution to be developed

7 - Practitioners' Community leaders

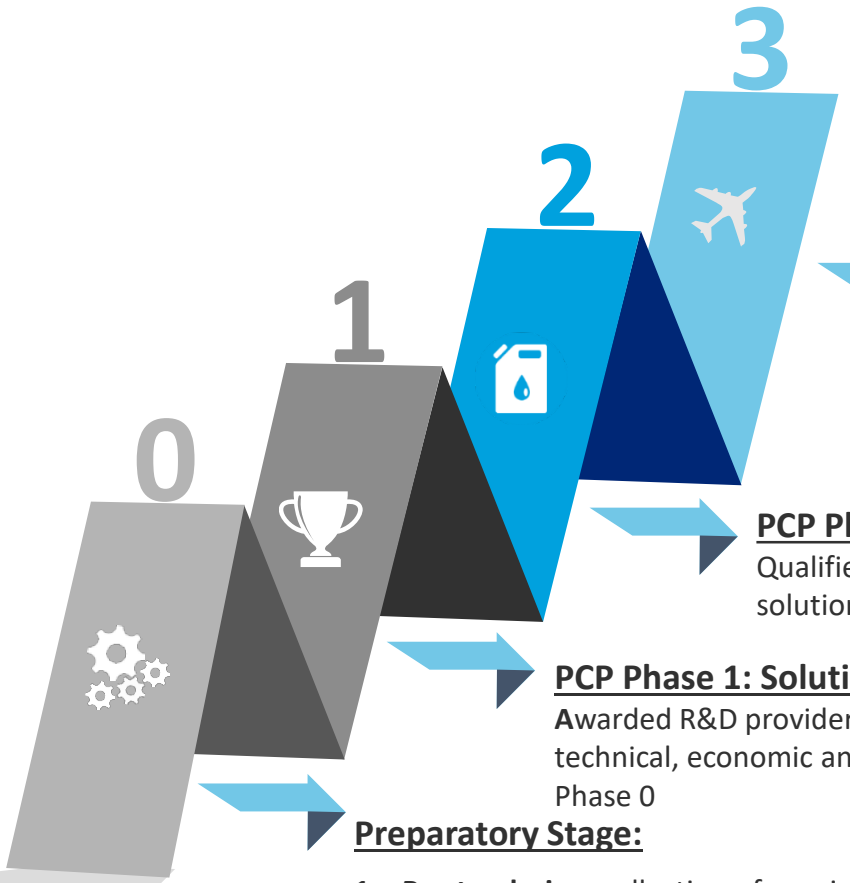
Organizations operating in public transport and homeland security domains, holding a large network base of subscribers from the public transport. **UITP**, **PPHS** and **ASSTRA** will be mainly responsible for building and managing the practitioners' community as well as communicating and disseminating information about ongoing project activities and achieved results

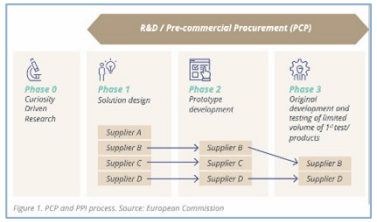
8 - Contractors

The successful bidders, selected by the buyer's group with the assistance of the Lead Procurer as result of the PCP call for tender. They will provide R&D services to the Consortium

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020374

Project Phases





PCP Phase 3: Operational Validation

At least 2 final solutions will be validated in operational environments in diverse conditions, using the scenarios and processes developed in the Verification and Validation Strategy

PCP Phase 2: Prototype Development

Qualified contractors will develop a first prototype based on the design documents delivered in the previous phase and test their solutions in lab conditions → focus on the creation of 4 prototype platforms from four different sources

PCP Phase 1: Solution Design

Awarded R&D providers are asked to describe the solution providing the complete architecture and design of the solution and verifying the technical, economic and organizational feasibility of their solution approach to address the PCP challenge, taking into account the results of PCP Phase 0

Preparatory Stage:

1. **Pre-tendering:** collection of requirements from the buyers' group methodology **/** Update of the state-of-the-art methodology / Business case / Open Market Consultation / common evaluation criteria / verification and validation strategy
2. **Tendering stage**: Tender publication & submission / Tender evaluation / tender award

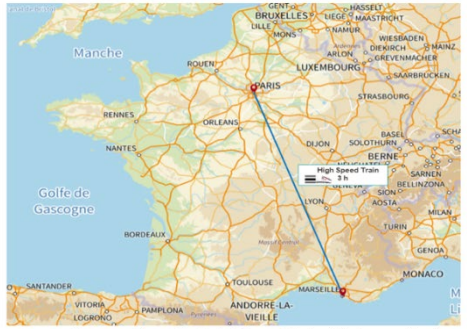
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020374

Pilots

France Pilot: Paris - Marseille axis

Involved partners: SNCF / RATP / REGSUD

Journeys between Paris stations with Public Transports



Journey from Paris to Marseille by High speed train

Portugal – Lisbon Pilot

Involved partner: ML

Oriente intermodal station **Platforms and lines** **Station Lobby**

Spain Pilot: Seville – Barcelona Axis

Involved partners: TMB / FGC / TUSSAM / SCC / INT / MIRPN

Italy – Genoa Pilot

Involved partners: AMT / ASSTRA

2020 res

Key takeways

- Market highly fragmented: security threats require highly sophisticated solutions, integrating technology innovations from different vendors;
- Often there is a miss-match between the users/demand and the supply side
- PCP puts together all relevant actors: users / suppliers / contracting authorities / domain experts
- PREVENT key success is based on the strong collaboration of different stakeholders
- Cross-boarder cooperation put at the heart: for gap analysis / common challenge / innovation procurement prototypes
- Help the supply side (SMEs and Large companies) bring innovation to market maturity

Where We Are

September - December 2022	Update SOTA and COTS analysis
January 2022	Open Market Consultations
June 2022	Tender publication
August 2022	Reception of Tenders, bidder selection and contract award
December 2022	PCP Phase 1 Solution Design (5 months)
May 2023	PCP Phase 2 Prototype (9 months)
February 2024	PCP Phase 3 Operational Validation (7 months)

Why join the UOG?

The User Observatory Group comprises experts and practitioners from public transport operators, Law Enforcement Agencies and security forces to ensure that the technology to be developed will fit the needs of the end users.

The practitioners who will be part of the User Observatory Group will be given:

- The chance to join a pan-European network of public transport practitioners and security services in order to exchange knowledge on public transport security.
- The possibility to follow closely the Pre-Commercial Procurement (PCP) process and get valuable inputs when it comes to procuring R&D services, including the regulatory and formal context (e.g. tender documents preparation, evaluating the tenders etc.).
- The possibility to learn and follow-up closely on technology innovation and R&D when it comes to public security innovations and prototypes. There are 4 prototype tests envisioned in the project, which means that practitioners will get to check how their remarks and input affects the final version and abilities of the prototypes.

Thank you for your attention!

Youssef Bouali

PREVENT PCP Coordinator
Senior Researcher & Project Manager
Engineering Ingegneria Informatica
phone: +39 338 6287919
e-mail: youssef.bouali@eng.it

info@prevent-pcp.eu

www.prevent-pcp.eu

www.twitter.com/PreventH2020

www.linkedin.com/company/prevent-pcp

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101020374

iProcureNet
Joint Cross-Border Public Procurement and PCP

Jozef Kubinec
Head of Works and ICT Procurement Department
Ministry of Interior, Slovak Republic

JOINT CROSS-BORDER PUBLIC PROCUREMENT AND PCP

Jozef Kubinec,
Ministry of Interior of the Slovak republic

Innovation by developing a European Procurer Networking for security research services

IPROCURENET

- Europe is producing high-quality, innovative security solutions, but never make it to the market.
- This is where procurers come in.
- **Procurers and procurement can act as a catalyst for innovation**.

IPROCURENET

ProcureNet aims to create an **ecosystem** of procurers, prescribers, legal advisors and other key stakeholders of security procurement, to

- share and analyse **security procurement trends and needs**
- **and open pathways for innovation in procurement** and joint procurement across EU member states.

IPROCURENET

In a three-cycle process, iProcureNet will

- map the European procurement environment,
- analyse investment plans,
- identify innovation needs,
- And develop **common and standardised practices** and a methodological framework for **joint cross-border public procurement (JCBPP).**

What we do in each cycle?

IPROCURENET

1. We compare investment plans
2. Based on it, we identify segments for possible JCBPP
3. We choose the most promising segment for JCBPP
4. We do market sourcing/market analysis of each segment

5. We conduct an online survey about JCBPP to collect examples of good practices.
6. As the final step, a joint procurement strategy for each segment is developed.
7. Based on joint procurement strategy, general methodology on how to conduct JCBPP is produced.

Online survey about JCBPP

THE ONLINE SURVEY

- The iProcureNet project conducted an online survey among European public procurers.

- The survey aimed to learn more about existing **JCBPP initiatives** throughout Europe
  - to collect examples of JCBPP
  - to identify good practices
  - and pitfalls to be avoided

FEEDBACK RECEIVED

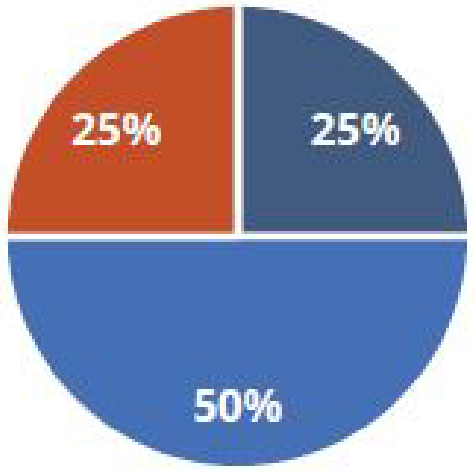
- An overall of **41 responses** from 14 countries (Germany, Ireland, Romania, Turkey, Estonia, France, Switzerland, the US, Portugal, Italy, Finland, Greece, Slovakia, and one unspecified) was obtained.

- The ten identified cases of JCBPP have been examined more thoroughly
  - Examples of PCP, PPI and also public procurement tenders

What we found out?

LACK OF EXPERIENCE BUT THE POSITIVE ATTITUDE

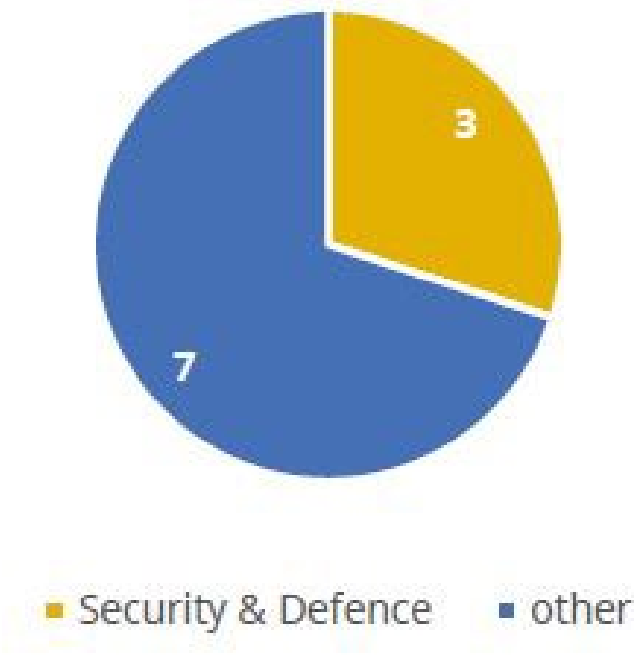
- Around 75% of the respondents had a **positive attitude towards JCBPP,**
- 25% had experienced it whereas
- 50% were interested or even planned to engage in JCBPP.



- Experienced JCBPP
- Consider JCBPP
- Not interested

FEW JCBPP EXAMPLES FROM THE SECURITY SECTOR

- From ten, three had experience in the field of security and defence



Good practices?

GOOD PRACTICE

- Building **motivated and available teams in the early stages of the project** is key to success.
  - For example, in the PPI4HPC project, it was decided, „even before the start of the project, to establish two working groups, one dealing with technical issues, one with legal issues."

- **Key stakeholders** should be identified and **support from senior management** ensured.
  - You will make mistakes and you need someone to turn to for support
  - JCBPP is a new thing and you need support

GOOD PRACTICE

- Procurement should be organized using **project-based management**
  - Dividing all actions into phases with deadlines and responsible person rules for information flow and decision-making (ex. vaccines in Estonia)

- **Functional specifications** should be preferred over technical specifications because they focus on long-term needs and **innovation**
  - It was mentioned when referring specifically to PCP, but it can also be applied to the public procurement tenders **to promote innovation.**

GOOD PRACTICE

- the need to **harmonize procurement practices**
  - For example, it can be good to start by **harmonizing procurement plans.**

- Tender Preparation Phase
  - Prepare an in-depth needs assessment and an **open market consultation** activity during the tender preparation phase.

- Tender Process
  - **Nominating a lead procurer** that already has longstanding relationships with all members of the buyer´s group proved a successful approach in HNSciCloud.

Open market consultation - space for innovation

OPEN MARKET CONSULTATION

- Physical and online meetings,
- Questionnaires,
- Presentations and testing of samples allow end-users to verify the suitability of the proposed solutions in real-life conditions,
- Less conventional methods, such as competitions, hackathons, idea markets

OPEN MARKET CONSULTATION

- Preliminary market consultation has several benefits such as:
  - for technical aspects:
    - Help in reviewing common and lot-specific requirements;
    - Improvement of definition and clarification of unclear requirements;
  - for legal and procedure aspects:
    - Conflict of laws during the procurement procedure;
    - Clarification on the application form

  *(**PPI4HPC** white paper "**Lessons learned on legal aspects**")*

DIFFICULTIES THAT HAD TO BE OVERCOME

Except for legal difficulties are there any other?

DIFFICULTIES THAT HAD TO BE OVERCOME

- Different **processes.**
  - There can be differences in procurement practices at the beginning of the cooperation.
  - Therefore, it is good idea to start by identifying different practices and harmonizing them.

- Different **language and culture.**
  - A common language should be agreed upon at the beginning of the cooperation.
  - In most cases, English is the first language (ex. procurement of vaccines in Estonia)

DIFFICULTIES THAT HAD TO BE OVERCOME

- The **coordination** among public procurers from different countries can prove to be difficult.
  - Organize frequent (weekly) telco

- agreeing on the **assessment process** and decision.
  - the evaluation part of the tender can present difficulties
  - especially when using functional specifications.
  - In the case of the **FABULOS** project, this issue was approached by setting up an **External Evaluation Panel** and the Technical Evaluation Committee.

BENEFITS OF JCBPP

Is it even worth it?

BENEFITS OF JOINT CROSS-BORDER PUBLIC PROCUREMENT

- The respondents have chosen the following **main benefits of JCBPP** from multiple-choice questions:
  - economies of scale;
  - possibility to negotiate better contract conditions;
  - promotion of innovation and R&D;
  - collaboration, sharing knowledge and exchanging good practice;
  - standardization of technical specifications.

BENEFITS OF JOINT CROSS-BORDER PUBLIC PROCUREMENT

- JCBPP can solve some of the problems specific to the health sector/security sector.
  - high level of confidentiality in the health sector
  - Different kinds of agreements for confidentiality are typical here
  - In the case of JCBPP for vaccines in Estonia, JCBPP had the effect of **revealing prices and opening up the market**

BENEFITS OF PRE-COMMERCIAL PROCUREMENT

- Public sector procurers can **compare the pros and cons of competing solutions**.
- IPR – **Risk/Benefit-sharing**
- **EU funding** of 90% is a clear benefit for cities.
- Appeals particularly to **SMEs and newcomers to the field**
- PCPs are one good way for cities to **solve societal challenges** that are too hard or too far in future to tackle with conventional procurement tools.

TIPS

TIPS?

The Preparation for JCBPP

Identification of joint procurement needs

↓

(Preliminary) Market research

↓

Identify financing opportunities & apply for funding, if neccessary

↓

Decision or memorandum to cooperate

↓

Collaboration agreement

↓

Preparing the technical description

↓

Choosing and drafting the terms of the procurement prodedure

In case of innovation consider:

* should the purchase include a pre-commercial procurement activity;

* should the stages of purchasing be arranged into one procedure or conduct two stages as separate procedures;

* should it be any negotiated procedure – competitive procedure with negotiations, competitive dialogue or the novel innovation partnership, a negotiated procedure without publication of a contract notice;

*terms of intellectual property rights

In case Defence and Security Directive might be applicable consider:

* the practice of Member States might be different concerning the applicability of the directive

* choise between restricted procedure and negotiated procedure with the publication of the contract notice

Next steps?

NEXT STEPS

- We are currently in second and third cycle.
- Focusing on the most promising segments only.
- Move from COTS to innovation – not possible by analyzing only investment plans.

NEXT STEPS

- We are going to lunch the next online survey in January 2022
- Share your experience with us and we will share examples of good practices with the buyers not only in the security sector

THANK YOU!

MGR. JOZEF KUBINEC, M.SC
HEAD OF WORKS AND ICT PROCUREMENT DEPARTMENT
PUBLIC PROCUREMENT DEPARTMENT
MINISTRY OF INTERIOR OF THE SLOVAK REPUBLIC

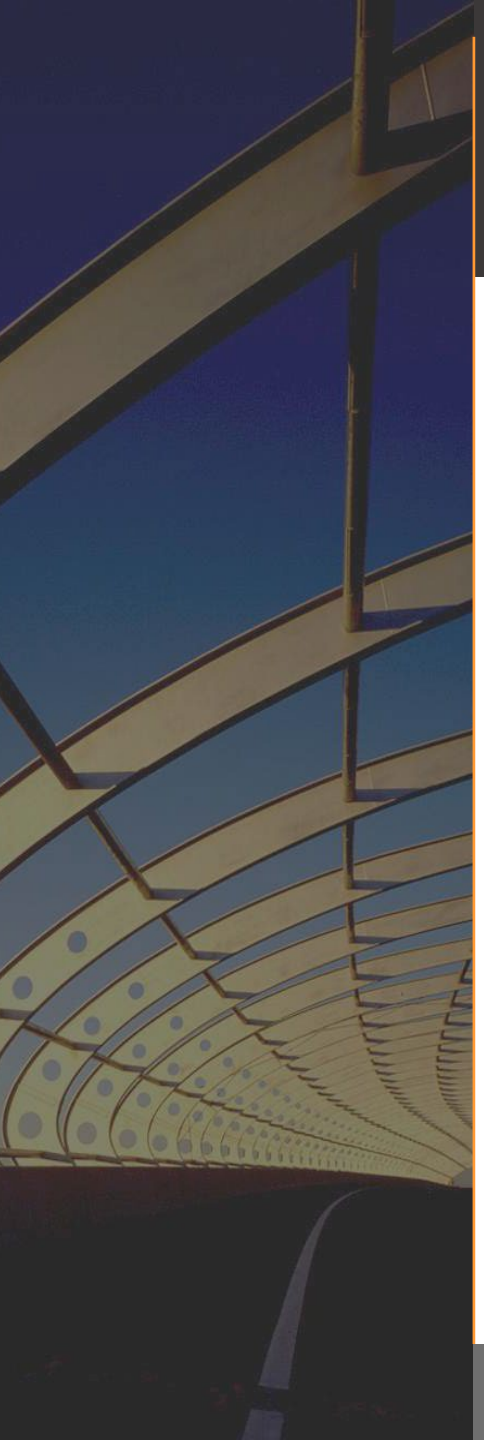
PRIBINOVA 2 | 812 72 BRATISLAVA SLOVAK REPUBLIC
PHONE: +421 2 509 44414 | MOBILE: +421 908 055 878
JOZEF.KUBINEC@MINV.SK | WWW.MINV.SK

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 32875.

Innovation by developing a European Procurer Networking for security research services

Q&A


COFFEE BREAK



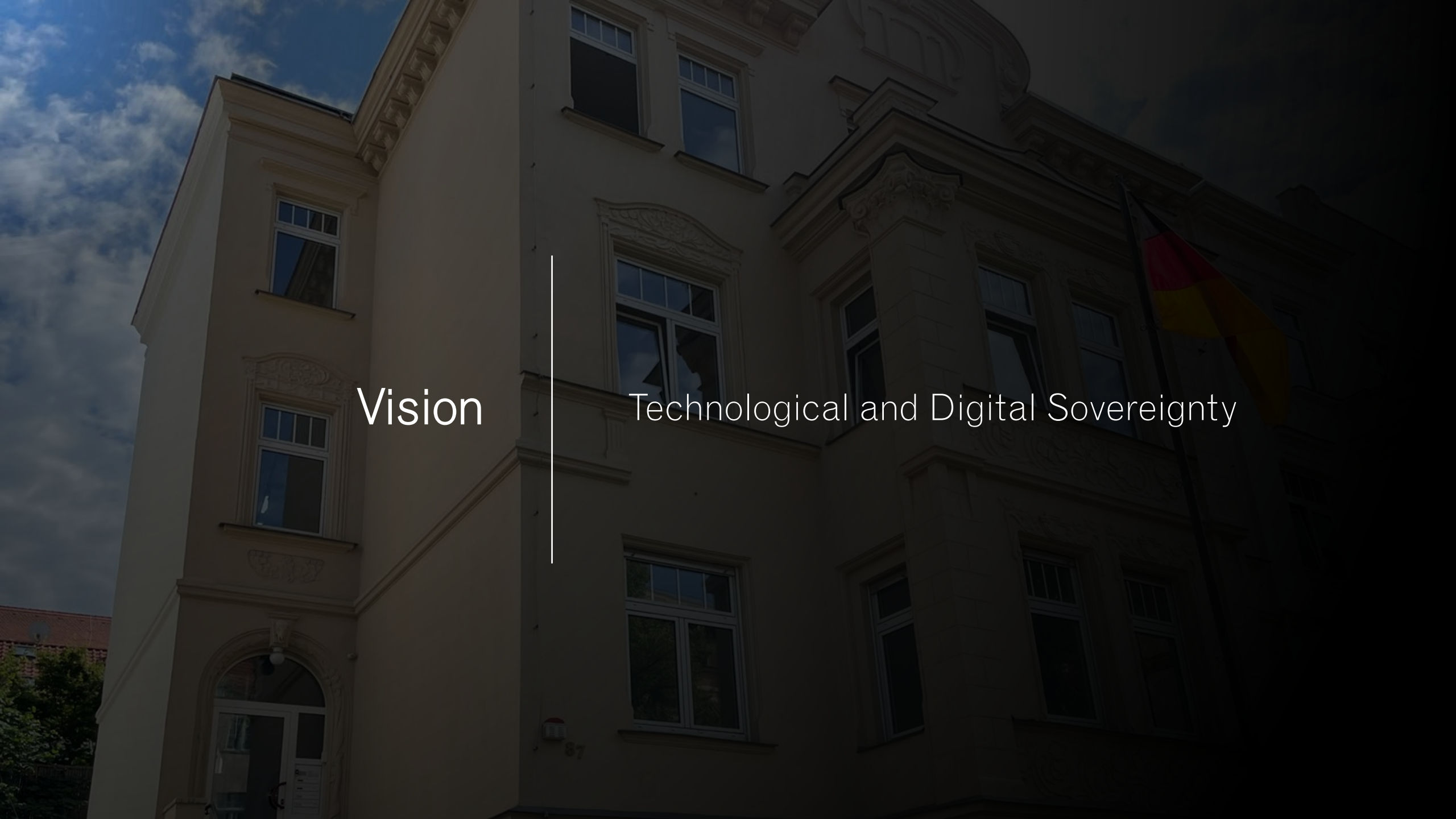
PART III

Cyberagentur
Human Brain Computer Interface (PCP)

Dr. Simon Vogt
Vicepresident
Cyberagentur, Germany

Dr. Simon Vogt

Agentur für Innovation in der Cybersicherheit



Vision

Technological and Digital Sovereignty

Mission

Initiating research and innovation projects for potential breakthrough technology in the domain of cybersecurity

Focus

High-Risk/High-Impact Research Projects

Method

- Targeted Innovation Challenges
- TRL 1-6
- Focus on Research Institutes, Universities, Research Companies


Enabling
Technologies


Secure
Systems


Secure
Societies

Organizational Challenges

- Deep Expertise Staff
- Trust Relationships with Researchers
- Focus on Research Institutes, Universities, Research Companies

Brain Computer Interfaces

- Direct Decision Transfer
- Control over Assisting Technology
- Secure BCIs

- PCP starting in Q2/22

Dr. Simon VOGT

Mail: vogt@cyberagentur.de
LinkedIn: Dr. Simon Vogt

www.cyberagentur.de
@CybAgBund

Cyber Innovation Hub
Dual use technologies launching customer (PPI)

Kor Gerritsma & Gertie Arts
Cyber Innovation Hub
Ministry of Defence, The Netherlands

CYBER INNOVATION HUB

'In service of Defence cybertopics, focussed on the business issues'

Cyber Innovation Hub

The cyber transformation engine for Defence

13 January 2022, eafip seminar

Kor Gerritsma & Gertie Arts

Microsoft Raced to Avert Cyber-Attack

By Kartikay Mehrotra and Alyza Sebenius

12 maart 2021 12:00 GMT

Defense One

TECH

With cyber organizatio devastatin

PUBLISHED MON, JUN 7 20
UPDATED MON, JUN 7 2021

Ryan Browne
@RYAN_BROW

SHARE

KEY POI

- It's still an believe qu
- In the U.K. in the age
- Quantum machines

Hacking

Russia attack

Microsoft s foreign org

Alexandra

Amidst th Headqua

BREAKING DEFENSE

Nakasone Warns Adversaries Unseen In US

"We should understand what our adversaries are doing," Gen. Nakasone are no longer launching attacks from different parts in the world. They u come into the US, use our infrastructure, and there's a blind spot for us them."

By BRAD D. WILLIAMS on March 25, 2021 at 5:48 PM

Gen. Paul Nakasone

WASHINGTON: Cyber Command chief Gen. Paul Nak America's adversaries are brazenly "exploit[ing] a gap

NEWS

New Report: The High Value of The North Sea

November 8, 2021

In the past land was distinguished from maritime territory by the presence of industrial and military assets that needed to be defended. This is no longer the case.

As the size, diversity and importance of sea-based assets and activities increase, whether it's windmills, undersea cables or offshore rigs , so do the entry points for criminal and terrorist actions, and for disturbances and attacks by state actors. As 'sea' becomes more like 'land', guaranteeing the security of structures and processes in the North Sea warrants more attention, and could potentially necessitate new approaches.

As an open economy and society, the Netherlands in particular is vulnerable not only to cyberattacks and disinformation campaigns, but also to hybrid threats to its maritime infrastructure. Its key position on the North Sea, means that its ports occupy a strategic

SPACENEWS

agency: Cyber attacks,

New York Times

govt

MIT Technology Review

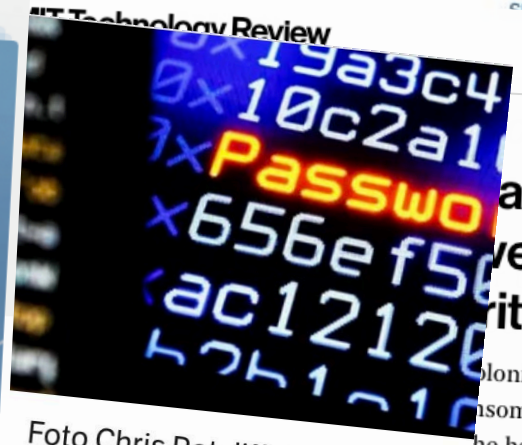


Foto Chris Ratcliffe/Bloomberg

ekt hulp bij
ups om
vallen af te slaan

eel Assistent
neraal NAVO

et gebouwd voor
gsvoering. Chef
ngen' David van

Subscribe

ansomware
veapon: self-
rity firms

olonial pipeline, two
nsomware victims. Then an
he hackers.

2021

Cyber Innovation Hub

Embedded in Defence

1. **Defence Cyber Strategy** (2018)
   'Invest in digital strike capability for The Netherlands'

2. **TNO Report** (2019)
   'Businessplan Cyber Innovation Hub'

3. **'Defensievisie 2035' & SKIA** (October/November 2020)
   'Vechten voor een veilige toekomst'

4. **National Cybersecurity Agenda (NCSA)** (2020)

*"**Cyber**, information and flexible, independent operational units need to have a prominent place in our armed forces."*

NLD Chief-of-Defence Onno Eichelsheim, Command-handover, April 2021

CYBER INNOVATION HUB

Vision & execution

Innovation guidance

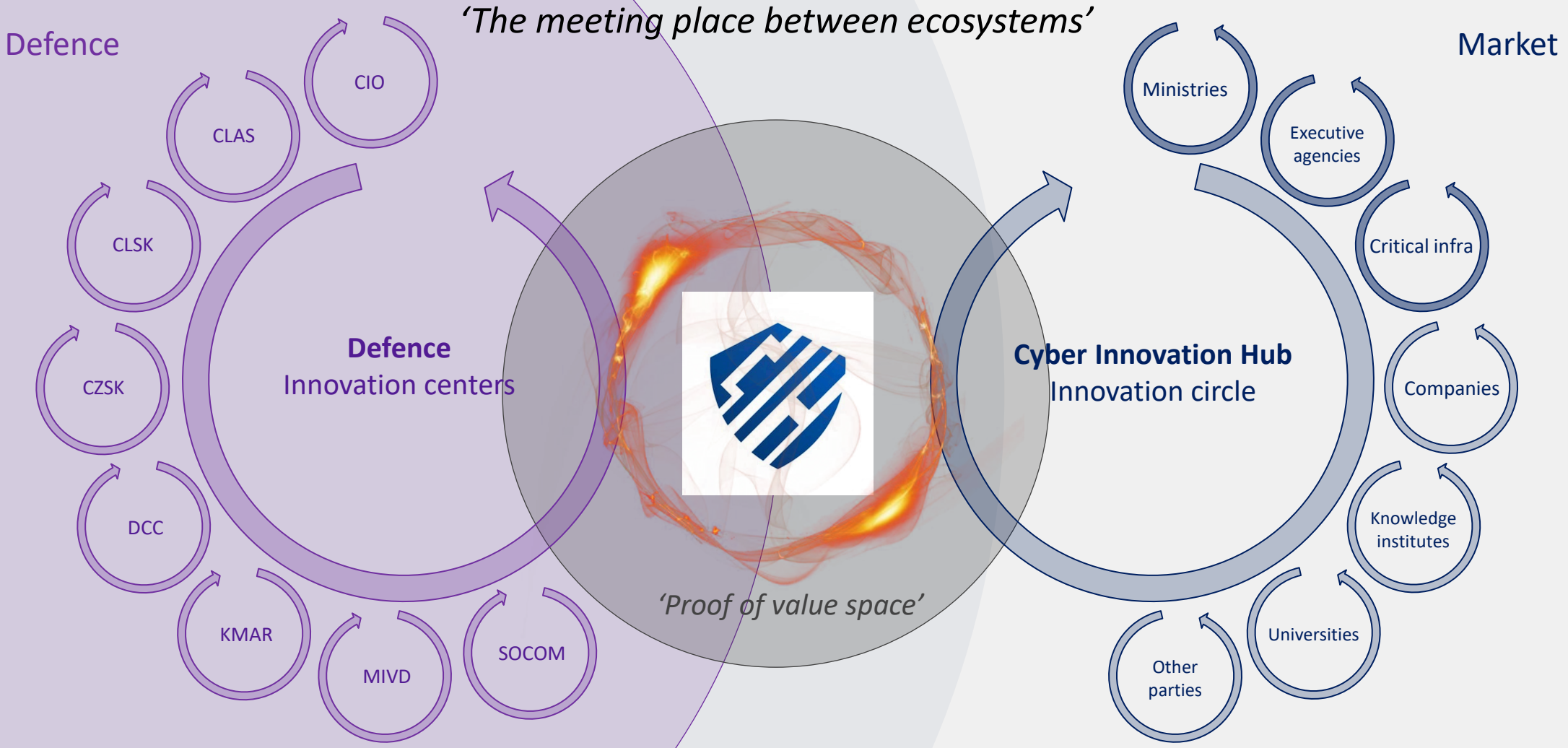
1. **Speed & agility**
   Accelerate speed and facilitate interactions with stakeholders

2. **Strategic collaboration & knowledge sharing**
   Building a high-end cyber community: strategic partners, interdepartemental & critical infrastructures

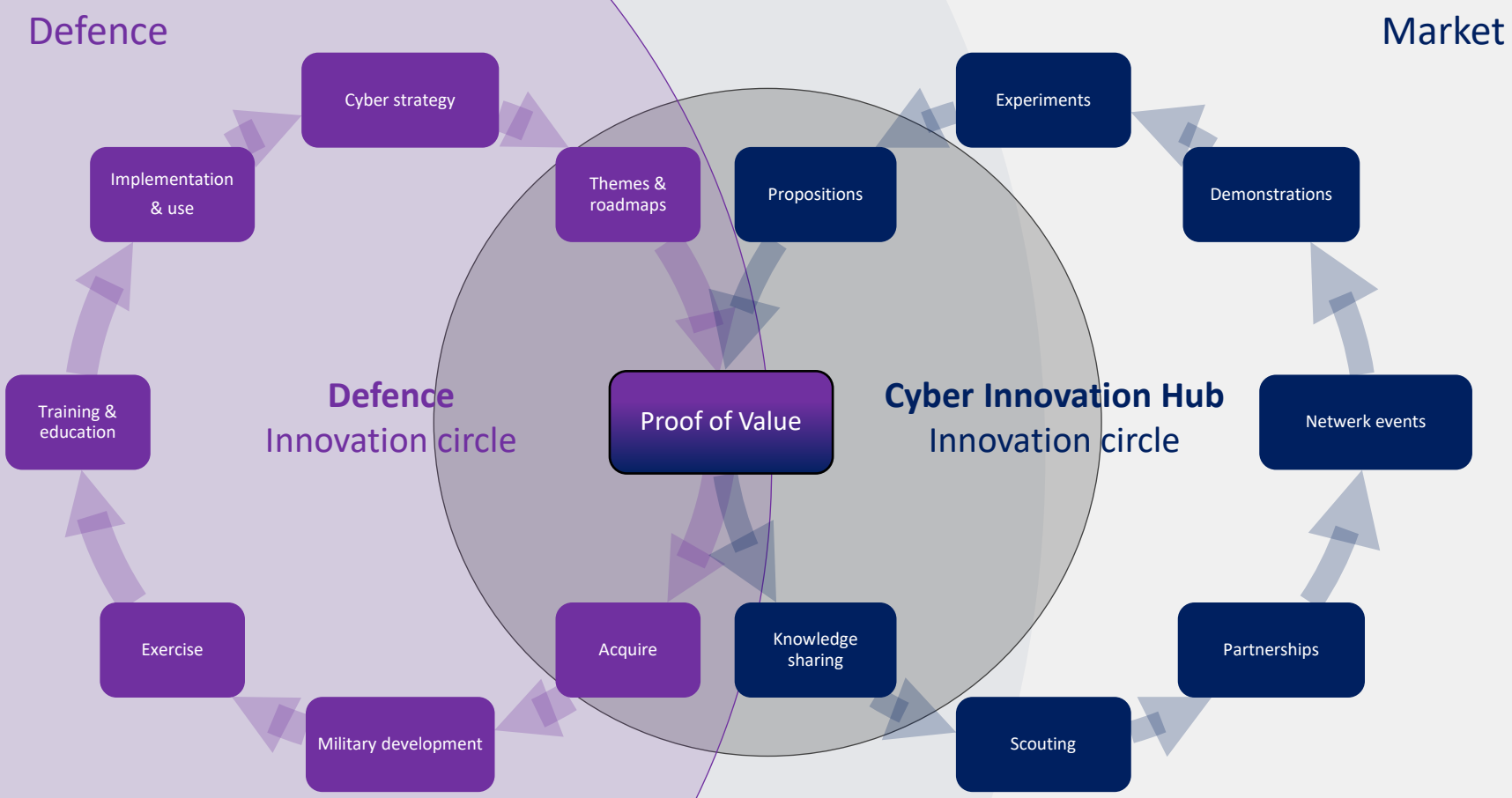
3. **Cross domain & Interdisciplinairy**
   Inclusion: whole range of cyberchain, synergetic combination of disciplines in projects

Cyber Innovation Hub

'The meeting place between ecosystems'

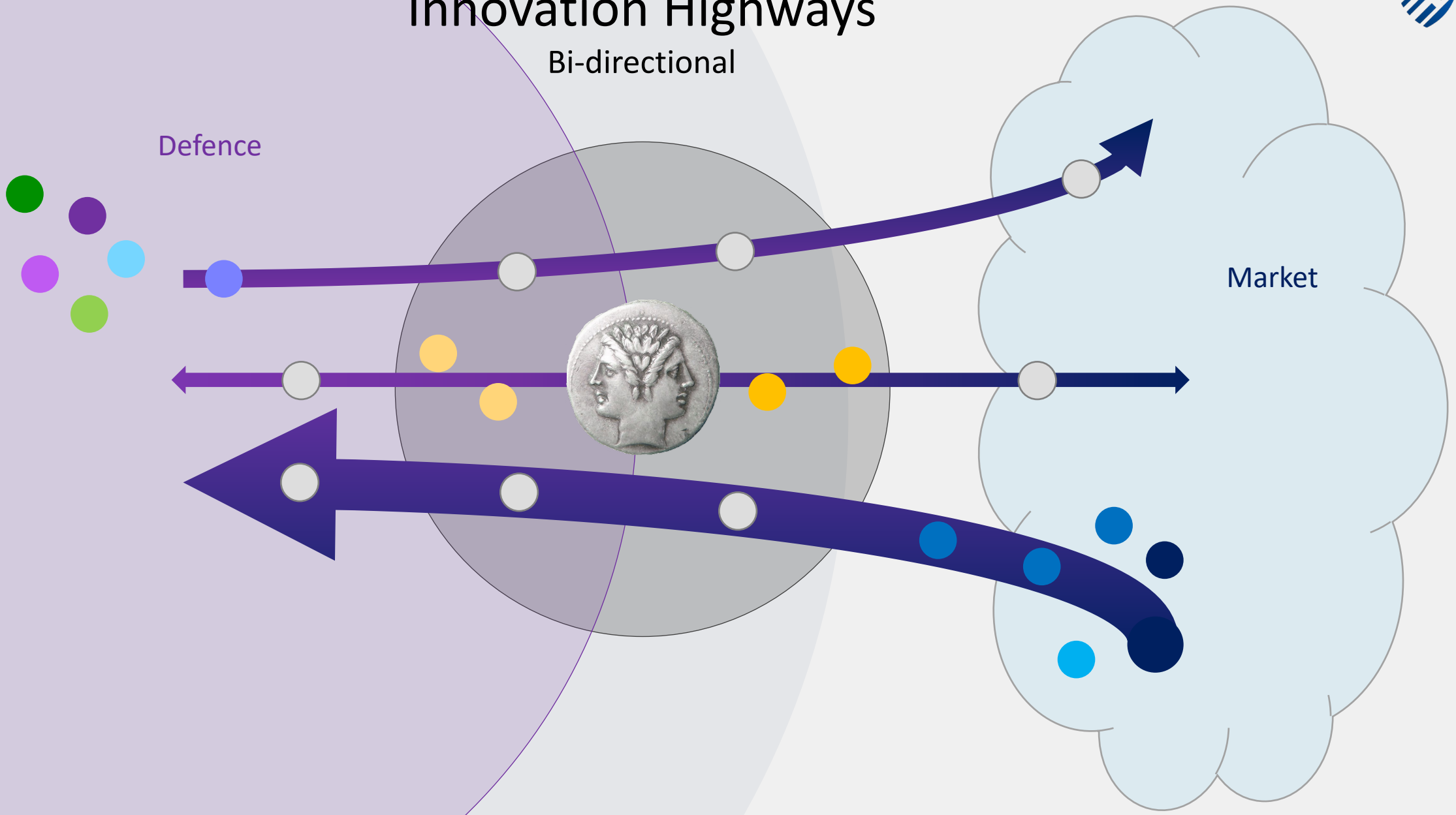


Complementary innovation circles



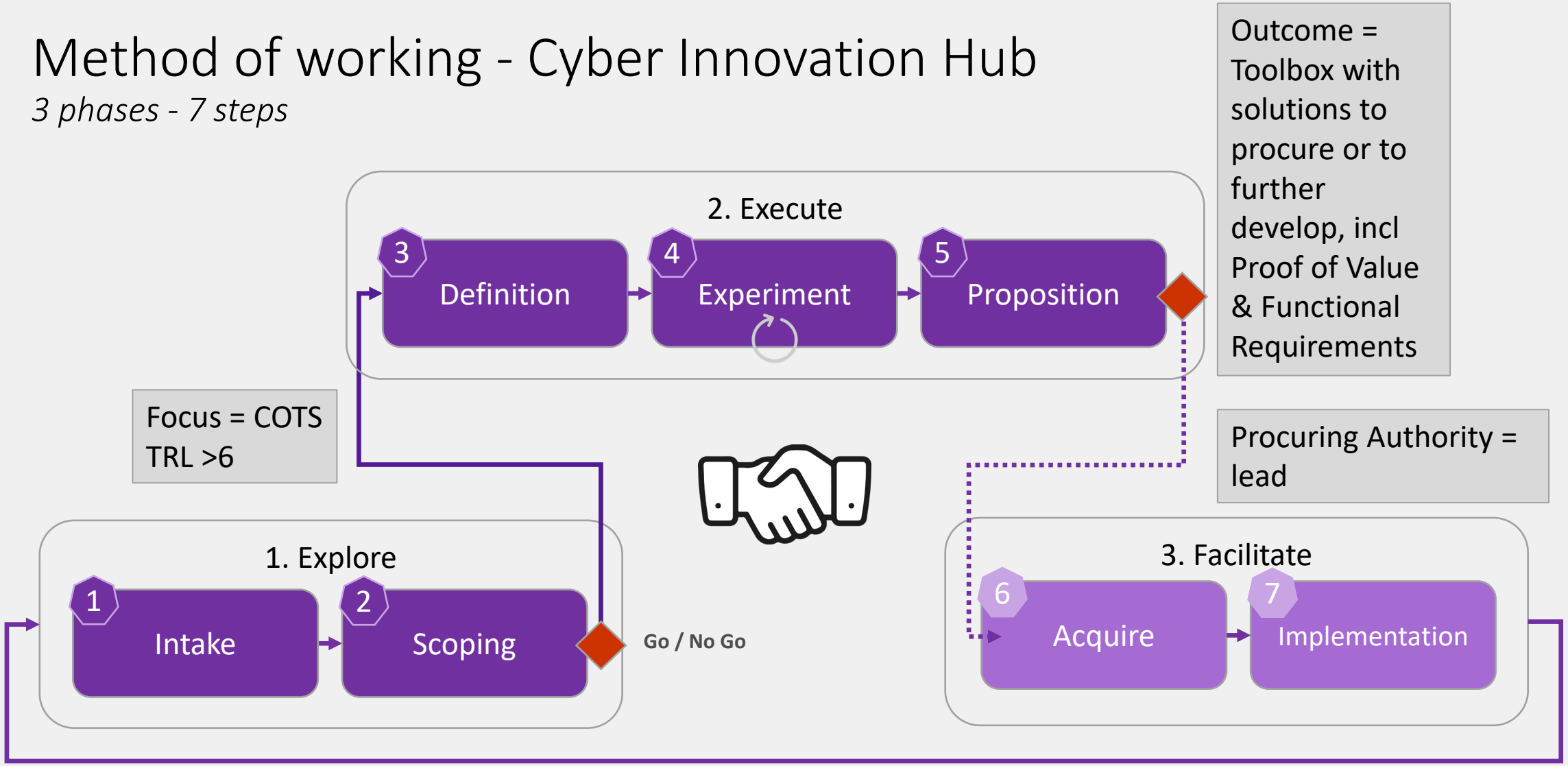
Innovation Highways

Bi-directional



Method of working - Cyber Innovation Hub

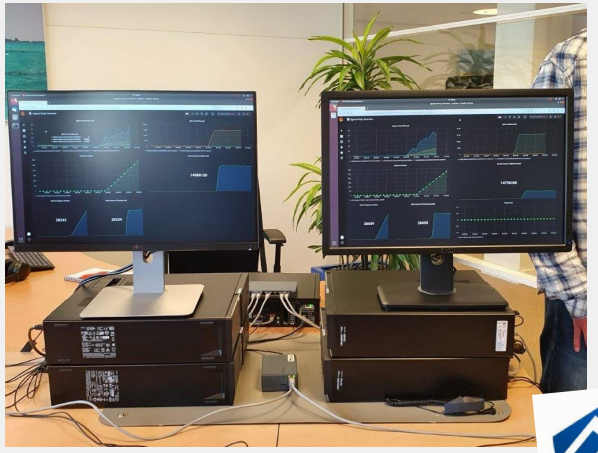
3 phases - 7 steps




powered by:
Cyber Innovation Hub
OSDD

Opensource datadiode (OSDD)

Example: NLD MOD development with market players

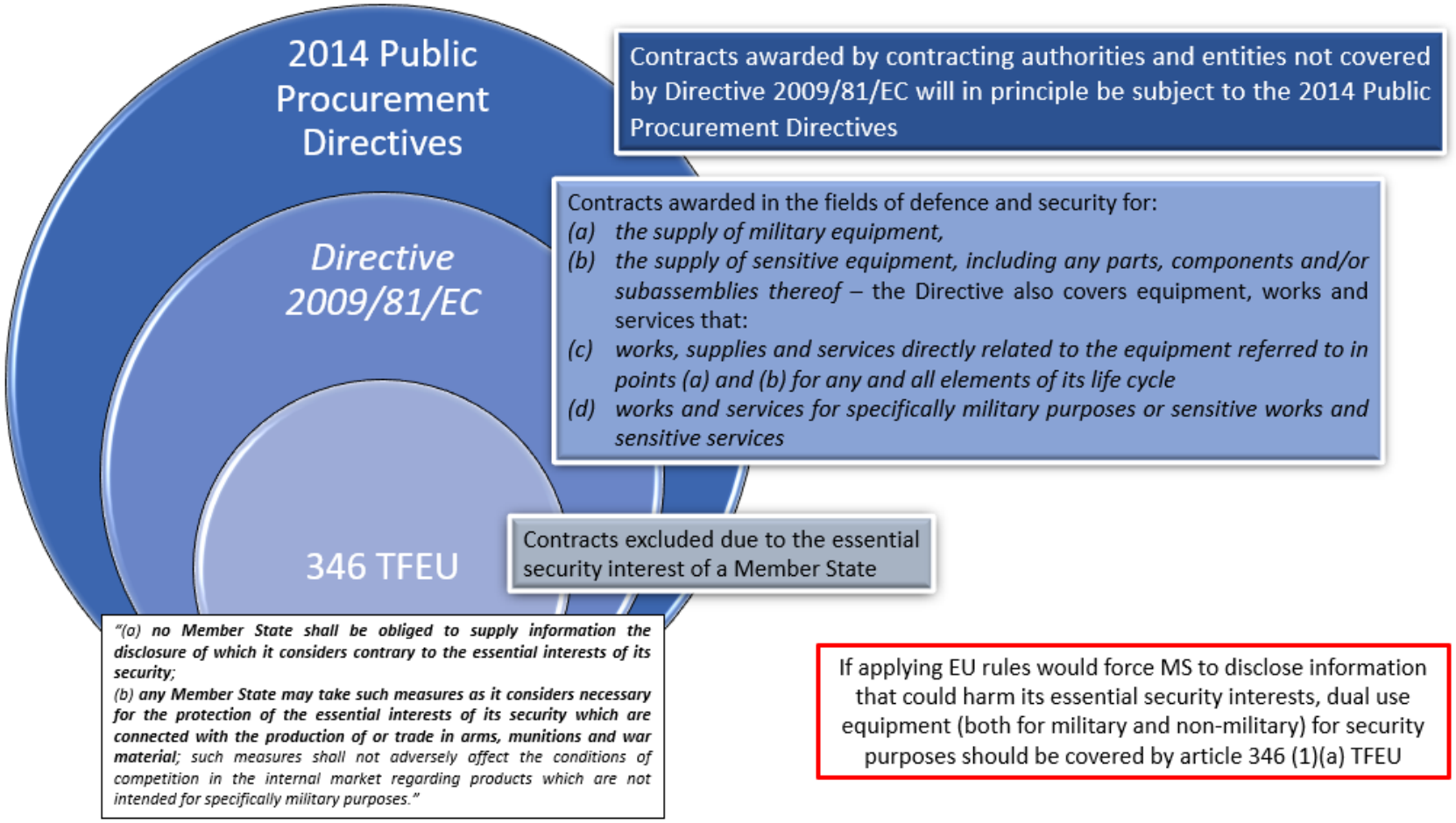


CHARACTERISTICS PROCESS:
- Speed
- Agility
- Collaboration

CURRENT:
- Experiments within Defence
- Experiments with Enexis
- Hackathon

RESULTS:
- Safety (depV)
- Cost reduction
- Broad interest for implementation

Different legal scenarios: What is allowed?



Transparency

DIRECTIVE 2014/24/EU

- Procedures for procurement by contracting authorities
- Public contracts above the thresholds

- Open procedure
- Restricted procedure
- Innovation Partnerships
- Competitive (negotiated) procedure
- Competitive dialogue
- Negotiated procedure without call for competition

Certain conditions

DIRECTIVE 2009/81/EC

- Contracts awarded in the fields of defence and security for: (a) the supply of military equipment; (b) the supply of sensitive equipment; (c) works, supplies and services directly related to points (a) and (b) for any and all elements of its life cycle; (d) works and services for specifically military purposes or sensitive works and sensitive services.

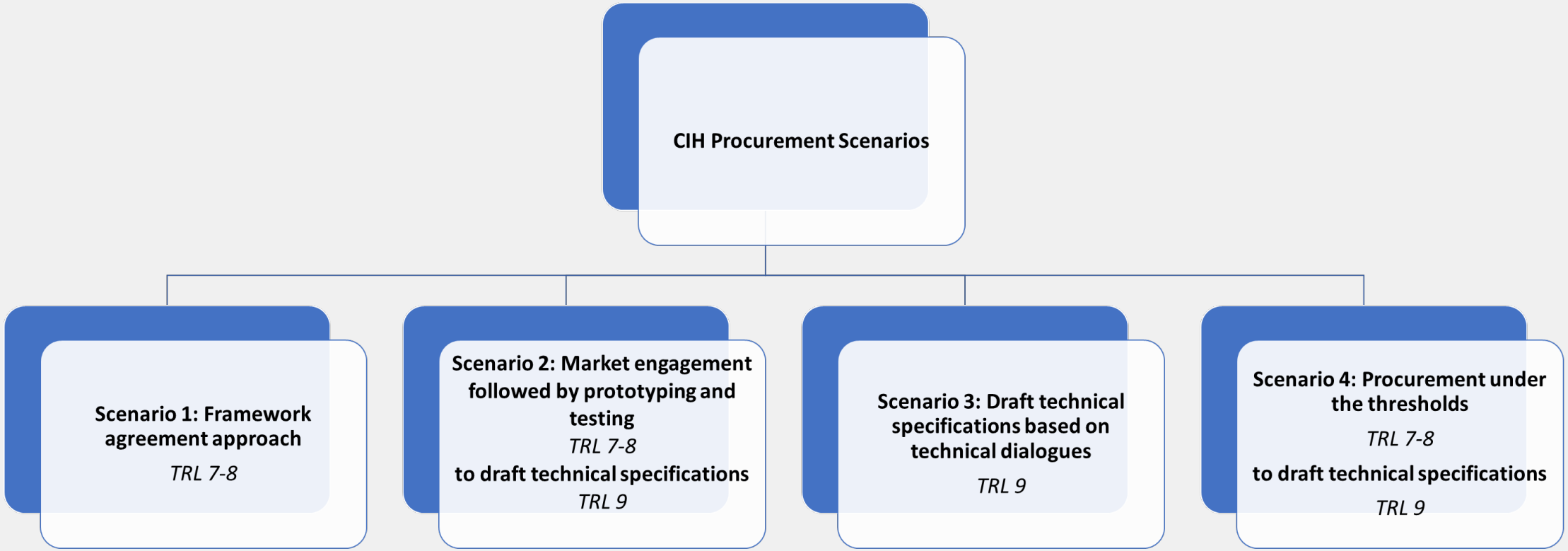
- Restricted procedure
- Negotiated procedure
- Competitive dialogue
- Negotiated procedure without publication of a contract notice

Certain conditions

346 TFEU

- Article 13 (a) Directive 2009/81/EC: Directive shall not apply to: *"contracts for which the application of the rules of this Directive would oblige a Member State to supply information the disclosure of which it considers contrary to the essential interests of its security."*

Scenarios in practice



Contact Information- Cyber Innovation Hub

CIH Lead
Wouter Roelofs

E: W.Roelofs.01@mindef.nl

CIH Operational Lead
Kor Gerritsma

E: KJ.Gerritsma@mindef.nl

CIH Strategic Advisor
Gertie Arts

E: GPW.Arts.01@mindef.nl

Public Procurement of Innovation and the National Cybersecurity Strategy: a Leverage Action for boosting Private Sector

Félix Barrio Juárez
Deputy Director for the Cybersecurity of Citizens
National Cybersecurity Institute, Spain

SPANISH NATIONAL CYBERSECURITY INSTITUTE

Public Procurement of Innovation and the National. Cybersecurity Strategy: a Leverage Action for boosting Private Sector

GOBIERNO DE ESPAÑA

VICEPRESIDENCIA PRIMERA DEL GOBIERNO

MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

017 TU AYUDA EN CIBERSEGURIDAD incibe_

Who we are

Spanish National Cybersecurity Strategy

Spanish National Cybersecurity Institute

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

CERT of reference in **cybersecurity** for citizenship, business, academy and strategic operators in Critical Infrastructures

National Digital Transformation Agenda

Citizens

incibe-cert_

Computer Emergency Response Team

Companies and professionals

What we do

Encourage digital trust

Provide support and incident response

Detect and promote cybersecurity talent

Promote the industry of the sector and innovation

Develop new technologies

Public Procurement of Innovation 2021-2025

- **Public Consultation to the Market for the definition of actions to promote cybersecurity through Innovative Public Procurement and the preparation of the Early Demand Map**

  - APRIL-SEPTEMBER, 2021
  - 1,005 M€ requested

Actions

R+D Programmes	SMEs Solutions	Strategic Operators	Public Sector	INCIBE Infrastructure	Talent & Training	Small projects
86,7 M€	24,8 M€	40,5 M€	30,4 M€	15,4 M€	20,0 M€	6,1 M€

INCIBE will carry out public procurement contracts for innovation in the next three years for a value of 224 million euros.

General Structure

GOBIERNO DE ESPAÑA | VICEPRESIDENCIA PRIMERA DEL GOBIERNO | MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL | SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_ SPANISH NATIONAL CYBERSECURITY INSTITUTE

***Note:** In this first phase of the initiative, INCIBE will be the Operational Manager, Contracting Body of the first challenges in Cybersecurity*

Governance levels	Strategic	Operational	Advisory
Participants agents	Dimensión interna	Task Network	
Participants bodies	SEDIA Comité Dirección INCIBE Comité intradisciplinar INCIBE	Designados por SEDIA WorkTeams *Task network*	Industry Public sector Academy and Research Experts pannels
Attributions / Functions	✓ Design, definition and validation of the strategy. ✓ Strategy monitoring. ✓ Definition of the early demand map and details of the tendering planning.	✓ Execution of the strategic initiative. ✓ Definition of the role of each actor in the deployment of the strategy and actions.	✓ Consultation with experts to introduce improvements in the definition and deployment of the strategy ✓ Publishing and dissemination of the actions. ✓ Creation of interest among the main actors.

Process

GOBIERNO DE ESPAÑA | VICEPRESIDENCIA PRIMERA DEL GOBIERNO | MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL | SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

incibe_ SPANISH NATIONAL CYBERSECURITY INSTITUTE

PRELIMINARY PUBLIC CONSULTATION

ACTION 1 | ACTION 2 | ACTION 3 | ACTION 4

PROPOSALS | PROPOSALS | PROPOSALS | PROPOSALS

BUSINESS

RESEARCH CENTERS AND UNIVERSITIES

START UPS

6 MONTHS

INFORME DE CONCLUSIONES

Early Demand Map

- Challenges and needs that can be resolved through CPI.
- Procurement plan.
- Defined budgets.
- Tenders list.
- Instrumentos de CPI.

2022

ELABORACIÓN DE PLIEGOS

PUBLIC TENDERS
One or more per Action

TENDER

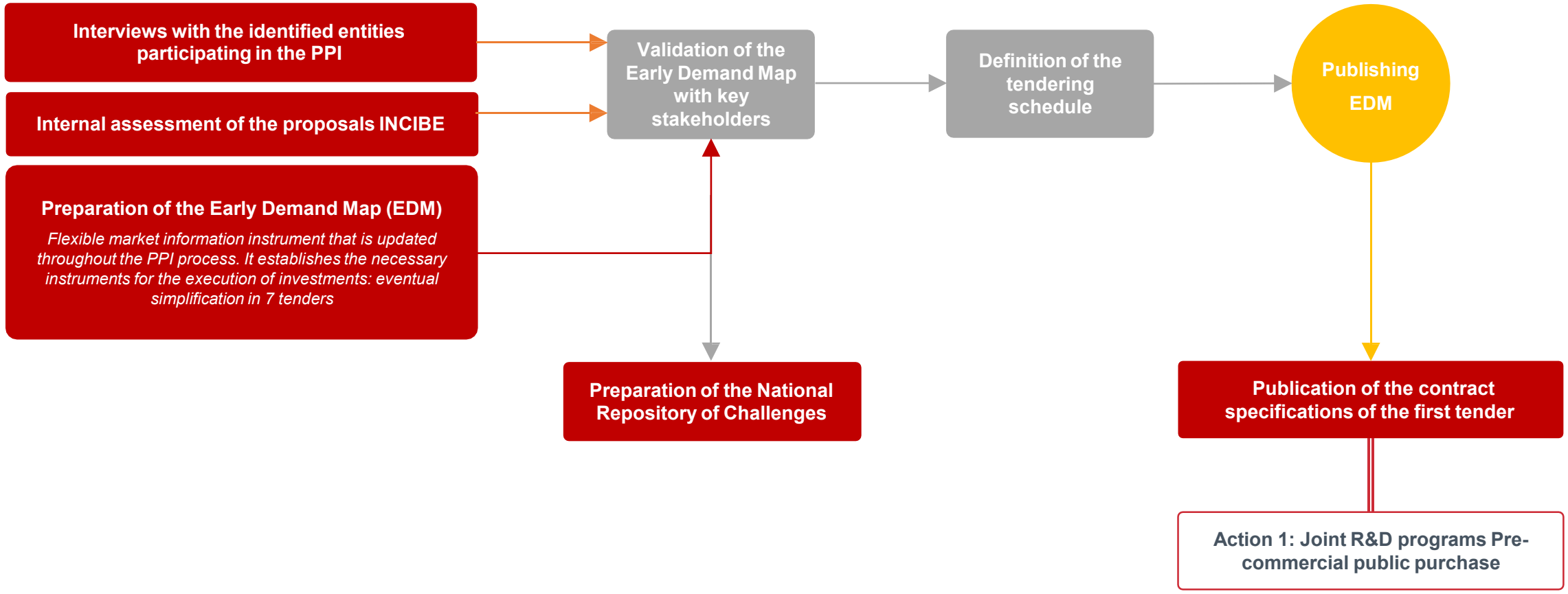
SUCCESSFUL CONTRACTORS

IPC CONTRACTS

- Same conditions for all the tenderers.
- Pre-comercial public procurement(CPP)
- Technology public procurement (CPTI)
- Consortia for Innovation (AI)

2022 - 2026

Next steps


Interviews with the identified entities participating in the PPI
Internal assessment of the proposals INCIBE
Preparation of the Early Demand Map (EDM)
Flexible market information instrument that is updated throughout the PPI process. It establishes the necessary instruments for the execution of investments: eventual simplification in 7 tenders
Validation of the Early Demand Map with key stakeholders
Definition of the tendering schedule
Publishing EDM
Preparation of the National Repository of Challenges
Publication of the contract specifications of the first tender
Action 1: Joint R&D programs Pre-commercial public purchase

Where to find us

Through our **channels:**

incibe_

Citizens

- OSI Oficina de Seguridad del Internauta — **Internet users**
- IS4K INTERNET SEGURA FORKIDS — **Children, parents and educators**

017 TU AYUDA EN CIBERSEGURIDAD incibe_

incibe-cert_ — **Incident Response Center**

Companies and professionals

- protege tu empresa — **Raising awareness for companies**
- ciber emprende — **Entrepreneurship in cybersecurity**

INSTITUTO NACIONAL DE CIBERSEGURIDAD

Thank you!

GOBIERNO DE ESPAÑA

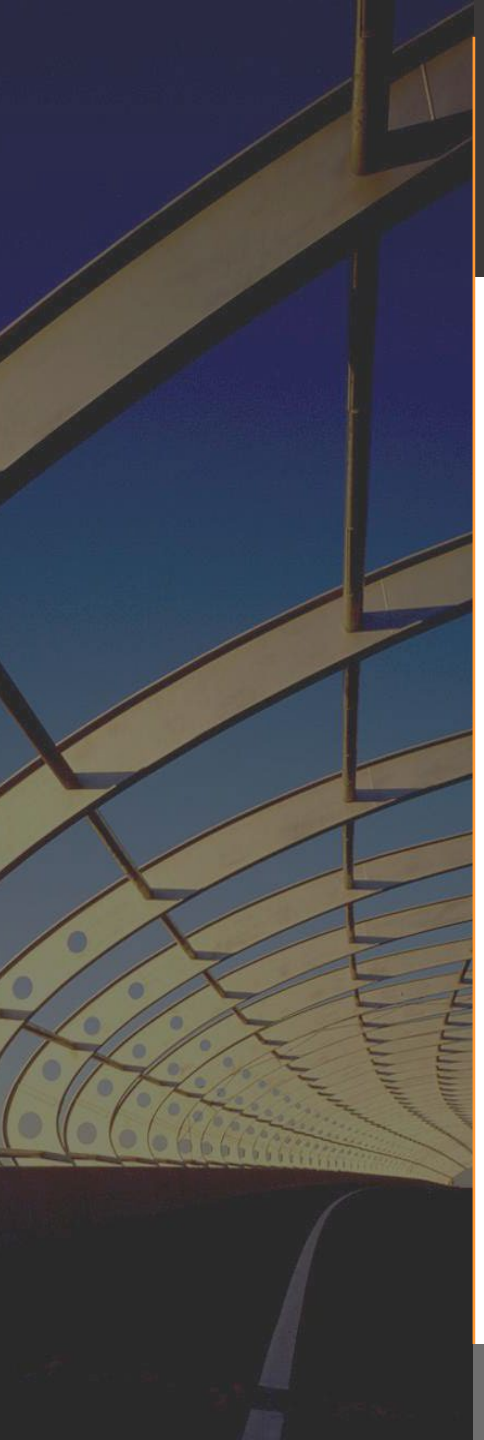
VICEPRESIDENCIA PRIMERA DEL GOBIERNO

MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

017 TU AYUDA EN CIBERSEGURIDAD incibe_

Q&A



Poll

Wrap up & Closure

Takeaways

- Public procurement can be a **strategic catalyst of innovation in the security domain** setting a win-win situation for procurers, suppliers and policy makers in order to get better products and modernize public services.
- The **procurement of cybersecurity innovations is a priority** towards EU strategic autonomy.
- Public procurers can act as **launching customers of dual-use technologies** that can be used for both civilian and military applications.
- Innovation procurement can **tackle common security challenges** in the transport sector.
- **Joint Cross-border Public Procurement** in security helps aggregate demand, reduce costs and steer innovation.

Future events

Topic	Date
Lessons learned from successful innovation procurement projects	15-02-2022

More information on: www.eafip.eu/events/webinars/upcoming-webinars/

1st CALL OF 2022 IS OPEN NOW!

Apply for free assistance

Deadline 15 April 2022

European Assistance For Innovation Procurement

eafip

https://ec.europa.eu/eusurvey/runner/EAFIP2022

Thank you for your attention

Corvers Procurement Services BV

The Netherlands

Tel: +31 73-612 6566

info@corvers.com

www.corvers.com

For any questions regarding EAFIP-Assistance and/or applying for free assistance, please contact:

Analucia Jaramillo

Tel: +31 6-20552773

a.jaramillo@corvers.com

www.eafip.eu

EAFIP WORKSHOP-WEBINAR #3

INNOVATION PROCUREMENT: CYBERSECURITY & DUAL USE

13 January 2022

Q&A

Part I

Insights into EU policy and trends

Speakers: David Rios Morentin (DG Home) and Aristotelis Tzafalias (DG Connect)

	Question	Answer
1.	**It seems that one of the main barriers is the fragmented security market in EU compared to what is happening in the United States for example. Is the EC is intentionally pushing to solve this issue? Are all actions in line to tackle fragmentation? Or is it just a side effect?** Question minute 27:29	That is one of the effects. The EC does not fund research for the sake of it, it funds research for the purpose to improve security to EU citizens. This is why new technologies to address security means, capability means are developed. The transition from research to operational stage is complex and there are many factors that can have a negative impact. Fragmentation is a very important factor. For example, not duplicating solutions, doing smart investments, bringing the demand together, having a stronger security market and a more competitive industry, and being able to provide technical solutions when and where they are needed are good ways to overcome fragmentation which is definitely, an important issue that the EC wants to address. As this is something that exists not only in the security domain, there is a strong effort and commitment by EC to bring all of us together.
2.	**We are all aware of the possibilities that PCP has to favour European development, in particular European technology providers and European SMEs. Is that also one of the EC´s focus areas? Is the EC also trying to have a positive effect or perhaps even to favour - if legally allowed - European companies?** Question minute 29:23	Of course, based on the rules of public procurement and trade rules, the EC wants to strengthen Europe´s industrial technology base. Europe has to improve our capabilities in many domains and also in security. Through public procurement, through innovation procurement, Europe needs to make sure that there is a demand, a consolidated demand, but also that there is a consolidated offer: to articulate the market, both sides are needed. Definitely, having strong European companies and strong European SMEs is very important for the EC because Europe needs this innovation capacity to sustain our capabilities, our security capabilities.
3.	**When is it expected that NIS 2.0 will entry into force?** Question minute 54:20	First, an agreement with the relevant stakeholder must be reached. On a first step, the proposal is developed. Secondly, the Council representing the Member States gives its opinion, followed by the European Parliament. Although the first NIS Directive took 3 years to reach agreement, there are reasons to be optimistic this time, since at the current stage all the relevant stakeholders are reaching an agreement.

		Only a couple of controversial aspects remain, so the odds are good. Once agreed, the proposal could reach a final agreement under the French presidency, so before June. After that a transition period, so there will be a year an a half or two for Member States to prepare and then for the entry into force, 2024 could be the entry into force and application of the NIS Directive
4.	**Public Procurement can play an important role, and as such our toolbox is wide when it comes to innovation procurement.** **The EU public procurement Directives from 2014 are widely applied by contracting authorities when implementing innovation procurement.** **However, are contracting authorities also using the instruments provided by the Defence Directive 2009/81/EC - which also applies to sensitive equipment and solutions – when it comes to security of supply chain and the technical requirements on Cybersecurity?** **I.e., is the audience using 2009/81/EC Directive for products and services related to dual use and critical infrastructure?** Question Poll minute 55:57	The results of the poll conducted during the workshop show that half of the participants have used the Defence Directive. The others are not aware of it. There is a clear need for alignment.
5.	**This question relates to the issue of technical requirements.** **From a procurement perspective, guidelines on technical requirements are very important but what would really help would be a fixed European wide understanding - if possible - on standards and standardisation. I.e., clear guidance on how to use these standards.** **Are the guidelines a first step to standardisation?** **There are a lot of discussions with contracting authorities about the possibility of excluding non-European**	When it comes to public procurement guidelines in the context of the NIS Directive, in some jurisdictions there is a centralised guidance regarding the language to be used, templates (for a Call for tenders for example), samples of clauses which also consider cybersecurity aspects. Since a public procurer has the mandate to ensure that the services, supplies or works purchased are safe, it is reasonable for that public procurer to ask how to translate this need for security in the tendering process. A reasonable expectation is that national authorities help their public procurement agencies to understand and express (cyber)security requirements, either as technical requirements or as part of service level agreements. For example, the energy department in the US has created templates of security related language to be used in contracts. In the field of security, and in particular in cybersecurity, the issue of trusted vendors and exclusions is critical. However, before

	providers from outside Europe. It would be simple very useful to have clear guidance in this regard from the European Commission. **Are the guidelines addressing issues happening in Europe regarding non-European telecom providers? Is the possibility of black-listing foreseen?**	even tackling this aspect, a lot of improvements related to the cybersecurity of products are needed. In this regard, standards play an important role. The CE is taking steps in this area and has recently announced a new initiative: the Cyber resilience Act. The initiative will be looking at the question of Cybersecurity in products and services. The issue of foreign providers goes a bit beyond the internal market into questions of national security.
6.	**There are a lot of differences from Member States on how they have implemented the NIS Directive in their national system, which is an issue to be tackled.** **From a cross-border perspective and for contracting authorities working together, harmonisation and understanding the common baseline is very important. Is it too soon or Member States can already take the initiative of a bottom-up approach in order to cooperate? Is this something that the EC would support?** Question minute 1:04:37	It is something that the EC will definitely support. Since the entry into force of the NIS (1) Directive (current one in force), two main opposed elements have been part of the discussions: • Sovereignty or national security. • The need to build trust between communities. In order to procure jointly, either innovation or Commercial-Off-The-Shelf technology, public administrations must, first and foremost, work together. In the Defence sector this is not happening as much as in other sectors. It would seem that EU level cooperation in and around civil cybersecurity is lagging behind, compared to law enforcement cooperation and military cooperation in the European context and in international organisations. The goal is to reach the same level of European cooperation in civil cybersecurity, but Member States push back, so an incremental approach to cooperation, information exchange and European level security procurement requirements has been preferred.
7.	**It is also interesting to see DG Home perspective. What do you think of this bottom-up approach to cooperate and to speed up this kind of cooperation?** Question minute 1:08:50	Many of the actions taken by the Commission and, in particular by DG Home, are oriented to improve cooperation between different stakeholders and communities. It is true that there are different levels of heterogeneity in the different domains, for example, defence procurers and communities have longer tradition of cooperation and it is more structured. The civil security domain is learning from their practices and trying to structure the community and the cooperation among the EU security authorities in a better way. In fact, a lot of initiatives are taking place in this domain and improvements are being achieved. As the civil cybersecurity domain is even more heterogeneous than the defence sector, there is still no structured dialogue/communication between the demand and supply side as it already exists in the defence domain. The type of actors that intervene are much more diverse: public, private, corporate individuals, etc, which makes the dialogue more lively, but increases the complexity of bringing all the stakeholders

		together and find common interests. In this regard, several initiatives can be highlighted, for example the EU industrial strategies from 2020 and the 2021 update, the action plan for synergies between civil defence and space industries. All in all, not only bottom-up but also bottom-down coordination.
8.	**Have the projects and support from the Commission achieved their policy goals? Has political support increased sufficiently?** Question minute 1:11:29	The contribution that projects make to policy is a sort of uptake, a sort of exploitation of the results of research and innovation. Research and innovation take a long time, it does not happen immediately. Research projects have been launched for 14 years now. The Commission´s security program started 14 years ago. More and more results of past projects are becoming a reality in terms of products that origin in the market. For example, current state of the art technologies in the domain of fighting crime and terrorism, as well as border management. All the new systems used today are being provided by companies who at one point or another have passed through the Commission´s research program. I.e., the investment in research through the projects has contributed to new technologies that are increasing the security capabilities required by Europe´s policy priorities. It is a chain of action from a policy priority to establish an investment that is made, a development that is carried out by EU industry, and eventually some results and feedback to the policy. So yes, the projects are contributing to the policy the EU is putting forward. The fact that the Commission´s security program, the EU research and innovation in the security field exists for 14 years indicates something: We are now in a transition period, from H2020 to Horizon Europe with a civil security R&I budget of around 1.6 billion. There is continuity in terms of investment. There is a change in what is expected from the framework program. There is more and more trust in the outcomes of research. There is emphasis in what is going to happen after research is completed: how these research results are going to contribute to policy priorities, to security. There is an impact logic in the development of the new framework program. The EC is also keen to explore all avenues for uptake. There is meaningful support but that does not mean that the effort should decrease. It is important to keep working to demonstrate that this part of the research program is useful and that it contributes to the security of citizens.
9.	**How often Contracting Authorities in Member States use the exemptions from Directive 2014/24/EU or 2009/81/ES for procurement of solutions related to**	Currently the public procurement data from the EU Member States is heterogeneous and highly fragmented. However, a first deep analysis on the procurement practices of the Member States in the civil security domain is being done through an EU

	cybersecurity? For example, the exemption according to article 15 (2) of Directive 2014/24/EU.	civil security market study. The outcomes of this study will certainly help the Commission and the Member States in devising future actions to facilitate a more systematic and structured gathering of high quality national public procurement data from the Member States in the domain of internal security. But please note that civil security and cybersecurity are not exactly the same thing. See: CERIS – SSRI – EU Security Market Study (europa.eu)

Part II

State of play of European projects: MS working together in the transport area and iProcurenet under Horizon Europe Program

Speakers: Youssef Bouali (PREVENT PCP) and Jozef Kubinec (IProcurenet)

	Question	Answer
10.	**Europe has a fragmented civil security market. In the Prevent PCP project one way to tackle it is to have informative webinars in different languages. Can you say something about the engagement of SMEs not used to operate outside the national borders?** Question minute 1:39:17	Under the scope of Prevent PCP Project , there are some fresh findings in the last meeting in France where SMEs participated, in which they asked if there were high/taxing requirements for their participation in the tender. Companies indicated that there are many procurement tenders that require a big consortium because they lack economic capacity as they do not have high turnover numbers and they cannot participate even if they have very interesting solutions. But this is one advantage of PCP, that there are no limitations in that regard. In particular, the Prevent PCP Project does not ask requirements regarding commercial/operational deployment capabilities but only for the performance of R&D activities. Moreover, the Prevent PCP Project is reaching local players in their local languages, whom are not usually reached with usual tendering communication channels. This is possible thanks to local stakeholders and their active collaboration.
11.	**The iProcurenet project is considering a new methodology in order to have a common understanding on the new investments if any on innovation or products and solutions that are not already available on the market place.** **This is indeed a challenge, but can the iProcurenet project learn other projects such as the HPC project for example?** **What can be useful for the iProcurenet project methodology? What are other lessons learned - from e.g., Central Purchasing Bodies (CPB) working in 15 Member States or other Consortia – are useful for the iProcurenet project methodology? What kind of input is necessary to develop a new methodology?** Question minute 2:03:48	These are all very good ideas as projects such as the iProcurenet project are research projects, so the learning curve is exponential. It is already clear that investment plans are not necessary the best way to identify innovation needs. And consequently, other methods and methodologies are going to be added. The iProcurenet project is also going to look into how CPBs in different countries are actually analysing the needs of their end users, i.e., the buyers. In fact, there is one project in Austria in collaboration with the European Commission which organizes seminars for CPBs. The iProcurenet project is planning to contact them to learn about their methodology. See also the iProcureNet Report: iProcureNet_JCBPP-survey_Feb21.pdf

12.	**How do you propose to increase the professionalization of public buyers? Are CPBs useful in this regard?**	There are several means how to increase the professionalization of public buyers. • The iProcureNet online survey respondents have chosen the main benefits of joint cross border public procurement (JCBPP): collaboration, sharing knowledge and exchanging good practices. In this sense, it seems that public buyers' cooperation during JCBPP increases the professionalization of their procurement experts. • Organizing workshops to share knowledge and exchange good practice is another way to increase professionalization. For example, a joint workshop on innovation procurement was organized together with MEDEA, CIVILnEXT and iProcureNet on 30th of March 2021. The objective was to offer a short course/training about innovation procurement and help practitioners acquire security solutions adjusted to their needs. • Implementing one tender through a CPB instead of several tenders by each public buyer means overall lower administrative costs and staff capacity. The centralization of purchasing should also bring with it an increase in the professionalization of procurement. This idea is expressly confirmed by the Directive 2014/24/EU, which states in Article 69 - "In view of the large volumes purchased, such techniques may help increase competition and should help to professionalize public purchasing ". The benefits of professionalizing public procurement by CPBs are apparent. It will be less demanding for a more experienced CPB to prepare tender documents and be more efficient within the general procurement process. There is also a smaller risk of procedural errors, due to the professionalization of the staff, which means fewer audit procedures. Additionally, CPBs may afford to offer more competitive salaries to purchasers who specialize in purchasing a particular commodity, e.g., computer technology, drones or ballistic protection. The study on how JCBPP is done through CPB (for example, FRONTEX if possible) will be conducted in the following cycles of iProcureNet. The initial hypothesis is that some public buyers from the security sector would welcome a European CPB in the security sector due to the current complicated system of using EU funds, with long-time audits of all tenders financed with EU funds.
13.	**Why drones can fly over water reserves, should not they be banned in all European countries?**	It could be due to different national regulations for safe operations of drones. National aviation authorities may state where drone operations are forbidden.

		For more information, please contact the European Union Aviation Safety Agency.
14.	**When are these workshops by BBG taking place? Is there more information available?**	The workshops are part of the Public Procurement Excellence Programme 2021, implemented by the Austrian Federal Procurement Agency (BBG) and the Vienna University of Economics and Business (WU). Application for next 2022 edition will be open during summer 2022. For more information, please visit https://ppe.bbg.gv.at/

Part III

Llessons learned and complementary approaches in three Member States. How to tackle the challenges in Cybersecurity: the German, Dutch and Spanish perspective.

Speakers: Simon Vogt (Cyberagentur), Kor Gerritsma and Gertie Arts (CIH -NL Ministry of Defence), Félix Barrio Juárez (Incibe)

	Question	Answer
15.	**It is interesting to see that such a young organization like Cyberagentur is so enthusiastic on the path forward on PCP.** **It has also been pointed out that selecting the right procurement strategy heavily relies on the State-Of-The-Art analysis per dossier/project. Additionally, one the lessons learned of R&D services is that the path is uncertain and also that the minimum requirements cannot always be set upfront. This is in fact one of the challenges that Innovation Partnership faces, since a public buyer needs to understand what the minimum requirements are before actually deploying the solution.** **However, this is not possible/straightforward at the lower TRLs (in a PCP for example).** **Can you say something about the foreseen budget for the PCP (conducted by Cyberagentur)?** Question minute 2:33:23	Cyberagentur´s yearly budget is around 65 million euro for research in general. The budget is allocated for the different topics. For the innovation challenge that Cyberagentur is currently preparing, the foreseen budget is around 10 million (but it also will depend on the number of participants). 10 million is the upper limit for all the different stages and for four or three different approaches in parallel. Nevertheless, money is not the issue here, the issue at stake is how to target the challenge and translate it for the market in the best way. That is the public buyer´s mission.
16.	**Is the Dutch Ministry of Defence/Cyber Innovation Hub using the exception regulated under Article 346 TFUE in a large number of cases?** Question minute 3:07:51	The Dutch Cyber Innovation Hub cannot share any data on this regard, since it is confidential. However, the Dutch Ministry of Defence does use the exception regulated under Article 346 TFUE and the Dutch Cyber Innovation Hub will probably make use of it for proof of concept in a security environment that is closed to the market. It is indeed a challenge to work with projects and products in an open environment, and in particular if this needs to be combined with the Article 346 TFUE regime.
17.	**On the Human Brain problem, does it raise a lot of ethical questions to take this approach?**	It does. But it is also a good example for the objectives of Cyberagentur, because it is a technology that will

	Question minute 3:10:25	develop and evolve anyways, and Cyberagentur can follow up and research on it. It is a technology that is currently in the edge of leaving the controlled labs and medical institutions and going to the consumer market. For this reason, Cyberagentur wants to introduce its own direct input in order to steer the market in the right direction and make sure the technology develops in a way according to Cyberagentur´s objectives. For example, in a way in which people and society interact with privacy aspects. The very first thing Cyberagentur undertook on this topic was to organize a public panel open for the public last autumn. The panel invited researchers from the field to discuss specially the ethical questions. The reason behind this initiative is to achieve not only a technology in a specific direction but also to raise awareness where necessary and also to gain trust when possible. The small pre-project that is currently carried out addresses specifically the privacy part. The technology is being anyway developed, but privacy and data security and cybersecurity for all BCI applications wherever they may come from in the future has to be ensured. This is the view Cyberagentur has on this topic and will continue to explain these topics and bring experts from all over the world to explain where the technology is going. Since the TRL is very low in many of the technologies Cyberagentur is interested in, the scope of future projects – with these ethical and social implications - is between 10 -50 years.
18.	**On the methodology of TRL, is it needed to have different approaches like System Readiness Levels (SRL), Integration Readiness Levels (IRL) instead of the TRL?** Question minute 3:29:18	In the context of Cyberagentur, these discussions have already been held within the company when setting up and discussing the strategy. The main question was whether TRL was a valuable and helpful method here. In the end, Cyberagentur chose it because it is the common reference in the field. I.e., if Cyberagentur indicates a particular TRL, most people would know the technology/project stage. Similar to the Dutch security field, in Germany there are different institutions in the whole innovation chain: 2 universities, different agencies tackling other topics (the man security issues) in innovations. All in all, luckily 7 or 8 institutions that go in hand in the whole innovation chain.

		Thus, TRL is a good reference measurement. However, in Cyberagentur´s projects the purpose/scope is considered first. I.e., there are limits and in some technologies is not even that easy to measure the TRL. Nevertheless, TRL gives a good reference and understanding of the concept, as long as it is not taken too strictly in a way that puts limits to a technology that is in development.
19.	**The number of tools that the EU Public Procurement Directives provide is large. From this tools, the exception under Article 346 TFEU is the least transparent and the most flexible one.** **It is clear that all the participants in the workshop are open to participation from for technology vendors from outside their country (hopefully from Europe, but sometimes even non-European countries).** **How has this been translated into the procurement approaches of the participants? For example, since the language issue is an specific barrier for SMES not used to work on that, is the local language or English used when publishing tendering documents? How is this being dealt with in the different countries?** Question minute 3:32:25	In the case of **the Netherlands**, the Cyber Innovation Hub has just been launched and the focus remains on Dutch companies. For the time being is mainly national, but in the future they will consider opening up participation to European entities. In **Germany**, the experience of the cyber innovation hub is similar to the one in the Netherlands. They start looking at German startups and looking at COTs in Germany, but there are other more recent projects that are also looking at vendors in Belgium because they are looking for the best possible solution. Since most of the organisations are still quite young, it is also a question of organisational development. The start should be as easy and most feasible as possible, opening up on a later stage and layer by layer for a broader scope. I.e., to go operational, start with a national scope, then EU level and then beyond. Nevertheless, for the Cyberagentur´s current project, the research community on the topic is so small and already so interconnected in Europe, that the starting field was already Europe. From the **Spanish perspective**, the goal is to solve main challenges and to differentiate agents within public and private agencies with different TRL. I.e., combining this strategy to have a global competitive market and an EU cybersecurity competitive industry but also working at local level to respond to the demand and supply that enhances these disruptive technologies challenges leading to a digital transformation.