

An aerial photograph of a city skyline, likely Shanghai, featuring a wide river with several large cargo ships and smaller boats. The city is densely packed with modern skyscrapers, including the Shanghai Tower and the Shanghai World Financial Center. The sky is overcast with soft, diffused light.

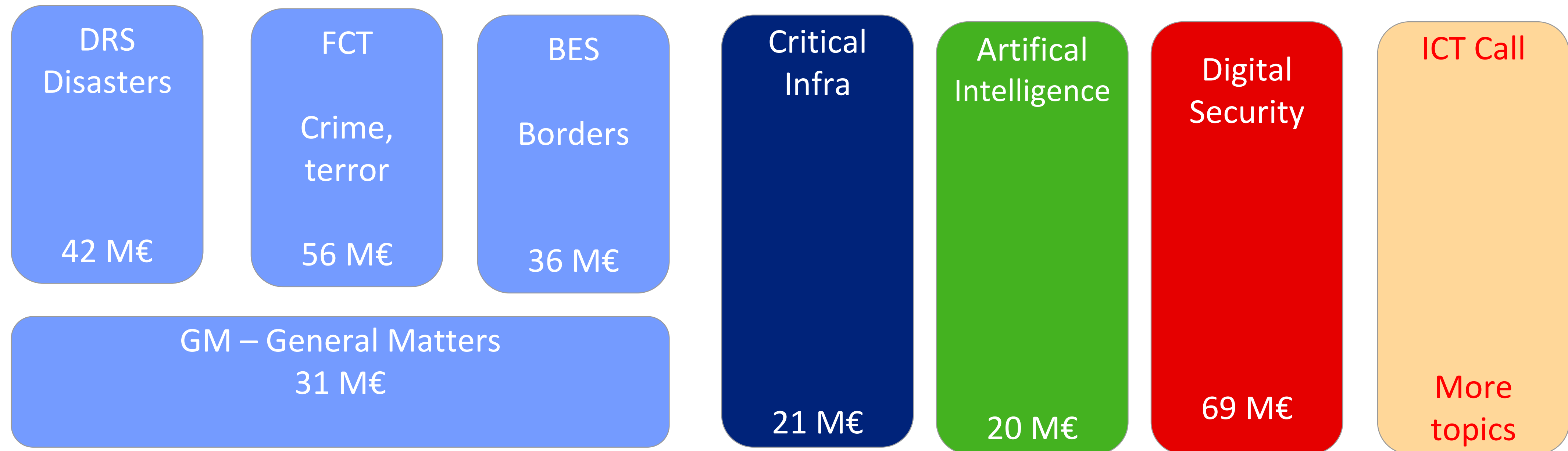
SECURE SOCIETIES CALL 2020

PAULI STIGELL
PEKKA RANTALA

BUSINESS FINLAND

8.10.2019

Secure Societies Call 2020



Last Call – 200 + 70 M€

BUSINESS FINLAND

Call	Topic	Topic	Type	SSH	Gender	Int.. Coop
INFRA	INFRA	01	IA	X		X
AI	AI	01	CSA			
	AI	02	IA			
	AI	03	CSA	X		
SEC	DRS	01	RIA	X	X	X
	DRS	02	RIA	X	X	(X)
	DRS	03	IA			
	DRS	04	RIA			
	FCT	01	RIA	X	X	X
	FCT	02	RIA	X	X	
	FCT	03	IA	X		
	FCT	04	IA			
	BES	01	RIA	X	X	X
	BES	02	RIA			
	BES	03	IA			
	GM	01	PCP			
DS	DS	02	IA/RIA	X		
	DS	03	IA	X		
	DS	04	IA			

Technology Readiness Level (TRL)

RIA

Research

- ~~TRL 1 – basic principles observed~~
- ~~TRL 2 – technology concept formulated~~
- ~~TRL 3 – experimental proof of concept~~

- TRL 4 – technology validated in lab

- TRL 5 – technology validated in relevant environment (industrially relevant environment in the case of key enabling technologies)

IA

Close to
market

- TRL 6 – technology **demonstrated** in relevant environment (industrially relevant environment in the case of key enabling technologies)

- TRL 7 – system prototype **demonstration** in operational environment

- TRL 8 – system complete and qualified

- TRL 9 – actual system proven in operational environment (competitive manufacturing in the case of key enabling technologies; or in space)

Sometimes this is not followed in Secure Societies Calls

Call - Protecting the infrastructure of Europe and the people in the European smart cities

SU-INFRA01-2018-2019-2020: Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe

- Innovation Action --- budget 20,7 M€, 7-8 M€ per project (3 projects),
- TRL→7
- Project length max 24 months
- At least **2 operators** of the chosen type of critical infrastructure operating in 2 Member States or Associated Countries must be beneficiaries
 - water systems, energy infrastructure (power plants and distribution, oil rigs), transport infrastructure (airports, ports, railways, urban multimodal nodes), communication infrastructures and ground segments of space systems, health services, e-commerce and the postal infrastructure, sensitive industrial sites and plants, and financial services.
- In 2020, while keeping the coverage of the assessment of risks, prevention, detection, response and mitigation of consequences, proposals should also address the **interrelations between different types of critical infrastructure** with the objective of developing tools and methods to minimise cascading effects and allow rapid recovery of service performance levels after incidents.
- When selecting for funding the proposals submitted in 2020, the Commission will take due account of similar projects financed in the previous years since 2016 (4 Calls).

Call - Protecting the infrastructure of Europe and the people in the European smart cities

- When selecting for funding the proposals submitted in 2020, the Commission will take due account of similar projects financed in the previous years since 2016 (4 Calls).
- <https://www.sauronproject.eu/> - ports, passenger ships ...
- <http://defender-project.eu/> - electrical energy (powerplants, grid)
- <http://www.resistoproject.eu/> - telecommunications
- <https://stop-it-project.eu/> - water supply
- <https://www.safecare-project.eu/> – hospitals
- <https://www.finsec-project.eu/> - banks
- <http://satie-h2020.eu/> Security of Air Transport Infrastructure of Europe
- <http://www.securegas-project.eu/> (coming soon) - Securing The European Gas Network
- <https://www.infrastress.eu/> - Improving resilience of sensitive industrial plants & infrastructures exposed to cyber-physical threats, by means of an open testbed stress-testing system
- *2019 results will be known in January 2020*

Artificial intelligence



New – AI in almost all Calls in 2020

3 topics (and 3 projects)

- SU-AI01-2020: Developing a **research roadmap** regarding Artificial Intelligence in support of Law Enforcement, CSA, 1.5 M€ (one project)
- SU-AI02-2020: Secure and resilient Artificial Intelligence **technologies, tools and solutions** in support of Law Enforcement and citizen protection, cybersecurity operations and prevention and protection against adversarial Artificial Intelligence, IA, 17 M€ (one project)
- SU-AI03-2020: **Human factors, and ethical, societal, legal and organisational aspects** of using Artificial Intelligence in support of Law Enforcement, CSA, 1.5 M€ (one project)

Call - Artificial Intelligence and security: providing a balanced assessment of opportunities and challenges for Law Enforcement in Europe

SU-**AI01**-2020: Developing a **research roadmap** regarding Artificial Intelligence in support of Law Enforcement

- CSA, 1.5 M€ (one project), 3 Law Enforcement Agencies (3 countries), 5 years
- Potential AI benefits for Law Enforcement Agencies (LEAs) are threefold, i.e., through:
 - 1) proactive policing (from reactive to anticipative policing);
 - 2) data analysis (e.g., connecting the dots, discovering criminal patterns and defragmenting LEA actions), and
 - 3) identity checks (improving detection, targeting and interdiction).
- Scope: Proposals under this topic should provide an **EU AI roadmap for LEAs**, meeting their specific operational and cooperation needs, by identifying, in a longer-term perspective: the key areas in which AI would be beneficial for LEAs, the key areas in which it could pose a threat to security, cybersecurity requirements for AI based technologies in use or to be used by LEAs as well as means of prevention and mitigation of malicious use of AI for criminal activities. As such this project would not only need to continuously interact (in a cluster mode) with projects funded under SU-AI02-2020 and SU-AI03-2020 but also **provide recommendations for further work to be done under Horizon Europe, Digital Europe, or the Internal Security Fund** as well as for policy and market uptake.

Call - Artificial Intelligence and security

SU-**AI02**-2020: Secure and resilient Artificial Intelligence **technologies, tools and solutions** in support of Law Enforcement and citizen protection, cybersecurity operations and prevention and protection against adversarial Artificial Intelligence

- IA
- 17 M€ (one project), 5 years
- 5 Law Enforcement Agencies (3 countries)
- Building on existing best practices such as those obtained through the ASGARD (<http://www.asgard-project.eu/>) and other projects, the project should establish a platform of easy-to-integrate and interoperable AI tools and an associated process with short research and testing cycles, which will serve in the short term perspective as a basis for identifying specific gaps that would require further reflection and development.

Call - Artificial Intelligence and security

SU-**AI02**-2020: Secure and resilient Artificial Intelligence **technologies, tools and solutions** in support of Law Enforcement and citizen protection, cybersecurity operations and prevention and protection against adversarial Artificial Intelligence

The image shows a screenshot of the ASGARD project website. The top navigation bar is blue and contains the ASGARD logo on the left and the following menu items: HOME, ABOUT, CHALLENGE & QUICK FACTS, CONSORTIUM, DELIVERABLES, RELATED PROJECTS (which is highlighted), WORK PLAN, and CONTACT. Below the navigation bar is a section titled "Public Deliverables" with a background image of a laptop keyboard and a calendar. Two document icons are displayed: "Design of the certification programme" and "Quality Management Plan". Below this is a section titled "Related Projects" featuring four logos: CPKIT, DANTE, IDENTITY, and ILEAnet (with the tagline "Innovation by Law Enforcement Agencies networking").

Call - Artificial Intelligence and security

SU-AI03-2020: **Human factors, and ethical, societal, legal and organisational aspects** of using Artificial Intelligence in support of Law Enforcement

- CSA
- 1, 5 M€ (one project), 2 years
- 3 Law Enforcement Agencies (3 countries)
- Proposals under this topic should provide an exhaustive analysis of human, social and organisational aspects related to the use of AI tools, including gender related aspects, in support of Law Enforcement, both for cybersecurity and in the fight against crime, including cybercrime, and terrorism. Points of view and concerns of citizens as well as of Law Enforcement should be tackled. Based on this analysis, proposals should suggest approaches that are needed to overcome these concerns and that stimulate the acceptance of AI tools by civil society and by Law Enforcement.

SU-DRS

Disaster-Resilient Societies



Resilience

4 topics – in all 8 projects

- SU-DRS01-2018-2019-2020: **Human factors**, and social, societal, and organisational aspects for disaster-resilient societies
- SU-DRS02-2018-2019-2020: **Technologies for first responders**
- SU-DRS03-2018-2019-2020: **Pre-normative research** and demonstration for disaster-resilient societies
- SU-DRS04-2019-2020: Chemical, biological, radiological and nuclear **(CBRN) cluster** ...

Disaster Resilient Societies

- SU-DRS⁰¹-2018-2019-2020: **Human factors, and social, societal, and organisational aspects for disaster-resilient societies**, RIA, 5 M€ (one project), 3 first responder organisation (3 countries)
 - Impacts: As a result of this action, Member States and Regional authorities as well as City and Metropolitan authorities should benefit from **recommendations and tools aimed at improving** the adaptability and preparedness of societies to different disaster risks
 - SENDAI; Co-funding opportunities from the **Japan** Science and Technology Agency (non-mandatory international co-operation)
- Call 2018 produced:
 - BuildERS Building European Communities' Resilience and Social Capital
 - RESILOC Resilient Europe and Societies by Innovating Local Communities

Disaster Resilient Societies

- SU-DRS02-2018-2019-2020: **Technologies for first responders**, RIA, TLR 6-7, 7 M€ (3 projects), 3 first responders' organisations (3 countries), Japan/Korea
 - Sub-topic 3: [2020] Methods and guidelines for **pre-hospital life support and triage**
 - Development of innovative tools, methodologies and European **pre-hospital guidelines for first responders of medical services, fire services and police and hospital trauma teams in order to ensure faster and more effective evaluation and control of numerous seriously injured casualties** in disaster and/or emergency situations. This should take account of lessons learned from military mass-casualty techniques such as damage-control surgery. The aim is to ensure more effective pre-hospital triage of victims with appropriate **digital traceability of actions and data transfer** from the event to the hospital(s), including across administrative and political boundaries.
 - Sub-topic [2020] **Open** – **5 first responders**

Disaster Resilient Societies

- SU-DRS03-2018-2019-2020: **Pre-normative research and demonstration for disaster-resilient societies**, IA, TRL 6-7, 6 M€ (one project), 3 first responders' organisations (3 countries)
 - Sub-topic 3: [2020] **First aids vehicles deployment, training, maintenance, logistic and remote centralized coordination means**
 - Improved standards and common communication data exchange mechanisms are required for an effective deployment of resources during the run-up to a major crisis related to any kind of disaster either natural (including resulting from climate-related extremes) or man-made, and immediately after the event, for example in case of a mass evacuation from an urban area. **Proposals should target in particular events where there are strong cross-sector, cross-border, cross-hierarchy coordination activities ongoing, and therefore the issue of interoperability.** The aim is to pave the way to improved standards, including voluntary Standard Operating Procedures (SOPs) and/or ISO or EN standards

Disaster Resilient Societies

- SU-DRS04-2019-2020: **Chemical, biological, radiological and nuclear (CBRN) cluster**, RIA, TRL 4-6, 3.5 M€ (3 projects), SME-lead

- In (2019 and) 2020 the Commission will select several RIAs aiming at research and **development of novel CBRN technologies and innovations identified in the catalogue that is updated by the ENCIRCLE project** on a regular basis. Each consortium implementing such a RIA must not only establish a consortium agreement among its members, but **also an agreement with the participants in the ENCIRCLE project** which must settle how the results from the RIA will be exploited and integrated into platforms managed by ENCIRCLE.



All beneficiaries of the RIA grant agreements must be independent from each beneficiary in the ENCIRCLE consortium (left)

<http://encircle-cbrn.eu/>

SU-FCT

Fight Against Crime and Terrorism



Fight against Crime Fight against Terrorism

4 topics – in all 9 projects

- SU-FCT01: Human factors, and social, societal, and organisational aspects to solve issues in fighting against crime and terrorism
- SU-FCT02: Technologies to enhance the fight against crime and terrorism
- SU-FCT03: Information and data stream management to fight against (cyber)crime and terrorism
- SU-FCT04: Chemicals: intelligence, detection, forensics

Fight Against Crime and Terrorism

- SU-FCT~~0~~1-2018-2019-2020: **Human factors, and social, societal, and organisational aspects to solve issues in fighting against crime and terrorism**, RIA, 5 M€ (2 projects), 3 Law Enforcement Agencies (3 countries)
 - Sub-topic 1: [2018, 2020] New methods to prevent, investigate and mitigate **trafficking of human beings and child sexual exploitation** – and on the protection of victims
 - Sub-topic 3: [2020] Developing comprehensive multi-disciplinary and multi-agency approaches to prevent and **counter violent radicalisation in the EU**.

Fight Against Crime and Terrorism

- SU-FCT02-2018-2019-2020: **Technologies to enhance the fight against crime and terrorism**, RIA, TRL 4-6, 7 M€ (4 projects)
3 Law Enforcement Agencies (3 countries)
 - Sub-topic 3: [2020] **Money flows tracking**
 - Sub-topic 4: [2020] Development and deployment of technologies, tools and relevant infrastructure to **identify speedily terrorist content online**, and prevent its re-upload
 - Sub-topic: [2018-2019-2020] **Open** - 5 Law Enforcement Agencies

Fight Against Crime and Terrorism

- SU-FCT03-2018-2019-2020: **Information and data stream management to fight against (cyber)crime and terrorism**, IA, TRL 5-7, 8 M€ (one project), 3 Law Enforcement Agencies (3 countries), 24 months
 - In 2020, proposals should address exclusively point b), with **a focus on private operators**. Although public authorities are primarily responsible for security, public-private cooperation is key in **protecting public spaces**. As an example, the first persons on the scene of a terrorist attack are often not police officers, but private security staff from local shops or transport operators. Moreover, public spaces are often owned and operated by private entities.

Fight Against Crime and Terrorism

- SU-FCT04-2020: **Chemicals: intelligence, detection, forensics, IA, TRL 6-7, 5 M€ (2 projects), 3 Law Enforcement Agencies, 36 months**
- - Criminals, including terrorists are constantly seeking new ways to develop, deploy and activate **dangerous chemicals (explosives, neurotoxins, new drugs, etc.)**. The way in which such chemicals can be manufactured and combined evolve continuously, which makes the specialized work of law enforcement agencies (LEAs) and reference laboratories in this area a continuous challenge.
 - Scope: Research needs to anticipate and match this challenge by
 - increasing the knowledge about these threats;
 - developing technologies to counter and respond to incidents with them,
 - improving knowledge on these dangerous chemicals and increasing deterrence messaging whilst also
 - recognising the need to minimise the inconvenience that security measures place on operators and users of public spaces.
- **Proposals have to demonstrate how they will effectively build on relevant previous H2020 projects and build synergies with on-going H2020 projects. (ENCIRCLE has good project lists)**

SU-BES

Border and External Security



3 topics – in all 7 projects

- SU-BES01 **Human factors**, and social, societal, and organisational aspects of border and external security
- SU-BES02: **Technologies to** enhance border and external security
- SU-BES03: **Demonstration of applied solutions** to enhance border and external security

Border and External Security

- SU-BES01-2018-2019-2020: **Human factors, and social, societal, and organisational aspects of border and external security**, RIA, 5 M€ (2 projects), 3 Border Guards Authorities (3 countries)
 - Sub-topic 3: [2020] Developing **indicators of threats at the EU external borders** on the basis of sound risk and vulnerability assessment methodologies

Border and External Security

- SU-BES02-2018-2019-2020: **Demonstration of applied solutions to enhance border and external security**, TRL 5→6, 7 M€ (3 projects)
3 Border or Coast Guards Authorities (3 countries)
 - Sub-topic 5 Disruptive technologies for non-intrusive identification of **hidden goods**
 - Detecting and identifying illegal goods hidden in containers, train cars and truck structures at EU external borders (e.g. **ports, wharfs, rail yards, ...**) is a need shared by border guard, customs and law enforcement authorities. **Illegal goods, including drugs, weapons, explosives, radiological and nuclear material**, are trafficked into Europe by criminal organisations using a range of methods and tools, which are very diverse (e.g. to minimize the risk of detection during transportation, some drugs may be transformed into a liquid and turned back into a solid at destination) and adaptable to specific border conditions. These may also include taking advantage of new technology to facilitate access to containers.
 - Sub-topic: [2018-2019-2020] **Open** - 5 Border or Coast Guards Authorities

Border and External Security

- SU-BES03-2018-2019-2020: **Demonstration of applied solutions to enhance border and external security**, IA, TLR 6-8, 5 M€
3 Border Guards Authorities (3 countries), 18 months, lead by civilian practitioner
 - Sub-topic 3: [2020] Improved systems for the **vessel tracking**, behaviour analysis and automatic anomaly detection
 - Solutions at high Technological Readiness Levels (TRL) to enhance border and external security need to be demonstrated in the context of actual operations or exercises for validation by practitioners. Part of Horizon 2020 activities related to border and external security for the period of 2018-2020 will be implemented by the European Border and Coast Guard Agency (EBCGA) in indirect management.
- Sub-topic: [2018-2019-2020] **Open** - 5 Border Guards Authorities

SU-GM

General Matters



General Matters

- SU-GM01-2018-2019-2020: **Pan-European networks of practitioners and other actors in the field of security**, CSA, 3.5 M€ (2 projects)
Practitioner participation from at least 8 Member States or Associated Countries
 - a. [2019-2020] Practitioners (end-users) in the same discipline and from across Europe
 - Option 1: **security and intelligence services**
 - Option 2: **fighting cybercrime**

General Matters

Practitioners (end-users) in the same discipline and from across Europe

- Option 1: security and intelligence services
- Option 2: fighting cybercrime

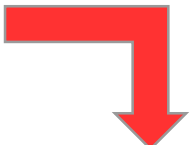
- Past

Acronym	Name	Type
eNotice	European Network of CBRNE Training Centres	a)
Fire-IN	Fire and rescue Innovation Network	a)
DARENET	DAnube river region Resillience Exchange networ	b)
ILEANET	Innovation by Law Enforcement Agencies networking	a)
I-LEAD	Innovation - Law Enforcement Agencies Dialogue	a)
ARCSAR	Arctic and North Atlantic Security and Emergency Preparedness Network	b)
EXERTER	Security of Explosives pan-European Specialists Network	a)
MEDEA	Mediterranean practitioners' network capacity building for effective response to emerging security challenges	b)
NO-FEAR	Network Of practitioners For Emergency medical systems and cRitical care	a)
PEN-CP	Pan-European Network of Customs Practitioners	a)

a) = same discipline

No overlap with current topic-options!

General Matters

- SU-**GM02**-2018-2020: **Strategic pre-commercial procurements of innovative, advanced systems to support security, PCP**
 - ~~Sub-topic 1: [2018] Common requirements specifications for innovative, advanced systems to support security~~ 
 - Sub-topic 2: [2020] Procurement of prototype systems among those specified as a result of Sub-topic 1. PCP, 24 M€ (based on 2018 CSA project's results)
- Participation is required of at least
 - 3 relevant practitioner organisations,
 - as well as of 3 potential "buyers" of systems
- Sub-topic 2 is only **open to entities having successfully participated in actions** under Sub-topic 1.

General Matters

- SU-GM02-2018-2020: Strategic pre-commercial procurements of innovative, advanced systems to support security, PCP
 - Sub-topic 2 is only open to entities having successfully participated in actions under Sub-topic 1. <https://prevent.eng.it>



General Matters

- SU-**GM02**-2018-2020: **Strategic pre-commercial procurements of innovative, advanced systems to support security, PCP**
 - Sub-topic 2 is only open to entities having successfully participated in actions under Sub-topic 1.
- iProcureSecurity Strategic Partnership of Emergency Medical Service Practitioners for Coordination of Innovation Procurement

<https://project.iprocuresecurity.eu/>

AT	JOHANNITER OSTERREICH AUSBILDUNG UND FORSCHUNG GEMEINNUTZIGE GMBH, SYNYO GmbH
BE	ASSOCIATION MEDICALE EUROPEENNE, JOHANNITER INTERNATIONAL
EL	Hellenic Society of Emergency Prehospital Care (HSEPC / EEEPF)
ES	FUNDACION PARA LA INVESTIGACION BIOMEDICA HOSPITAL INFANTIL UNIVERSITARIO NINO JESUS, SERVICIO MADRILENO DE SALUD
IE	THE PROVOST, FELLOWS, FOUNDATION SCHOLARS & THE OTHER MEMBERS OF BOARD OF THE COLLEGE OF THE HOLY & UNDIVIDED TRINITY OF QUEEN ELIZABETH NEAR DUBLIN
IT	Italian Resuscitation Council
TR	Ambulance and Emergency Physicians Association

SME INSTRUMENT & FAST TRACK TO INNOVATION

- Open topics
- The respective calls for the EIC-SME instrument (H2020-EIC-SMEInst-2018-2020) and EIC-Fast-Track-to-Innovation (H2020-EIC-FTI-2018-2020) are found under the Horizon 2020 Work Programme Part – ***Towards the next EU Framework Programme for Research and Innovation: European Innovation Council (EIC) Pilot***

BUSINESS FINLAND

Horizon 2020 Webinar
SC7/Cyber Calls In 2020
8 Oct 2019
Non-Confidential



CYBERSECURITY CALLS IN 2020 [2 July 2019]

Digital Security (BDG €69M)

- ✓ SU-DS02-2020: Intelligent security and privacy management
- ✓ SU-DS03-2019-2020: Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises
- ✓ SU-DS04-2018-2020: Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches

SU-DS02-2020: Intelligent security & privacy mgmt (1)

IA | EUR 2-5/2-5M | Opening 12 Mar 2020 | DL 27 Aug 2020

Specific Challenge: The increasing prevalence and sophistication of the IoT and AI broadens the attack surface and the risk of propagation. Need for tools to automatically monitor and mitigate security risks, including those related to data and algorithms.

Scope: Check: SU-ICT-03-2018 “Establishing and operating a pilot for a Cybersecurity Competence Network”. Sub-topic (a): Dynamic governance, risk management and compliance. Sub-topic (b): Cyber-threat information sharing and analytics.

SU-DS02-2020: Intelligent security & privacy mgmt (2)

RIA | EUR 2-5/3-6M | Opening 12 Mar 2020 | DL 27 Aug 2020

Specific Challenge: The increasing prevalence and sophistication of the IoT and AI broadens the attack surface and the risk of propagation. Need for tools to automatically monitor and mitigate security risks, including those related to data and algorithms.

Scope: Check: SU-ICT-03-2018 “Establishing and operating a pilot for a Cybersecurity Competence Network”. Sub-topic (c): Advanced security and privacy solutions for end users or software developers. Sub-topic (d): Distributed trust management and digital identity solutions & developing novel ID management.

SU-DS03-2019-2020: Digital Sec & privacy 4 citiz.&SMEs

IA | EUR 4-5/3-4M | Opening 12 Mar 2020 | DL 27 Aug 2020

Specific Challenge: Most Small and Medium-sized Enterprises and Micro Enterprises (SMEs&MEs) lack sufficient awareness and can only allocate limited resources - both technical and human - to counter cyber risks.

Scope: Sub-topic (a): Protecting citizens' security, privacy and personal data (innovative approaches, techniques and user-friendly tools). Sub-topic (b): SMEs&MEs: defenders of security, privacy and personal data protection.

SU-DS04-2018-2020: Cyb.sec+Electricity&Energy

IA | EUR 6-8M | Opening 12 Mar 2020 | DL 27 Aug 2020

Specific Challenge: The Electrical Power and Energy System (EPES) is of key importance to the economy, as all other domains rely on the availability of electricity.

Scope: The proposals should demonstrate how the actual EPES can be made resilient to growing and more sophisticated cyber and privacy attacks and data breaches. E.g. (i) assessing vulnerabilities and threats, (ii) designing adequate security measures, (iii) implementing resilience tests, (iv) demonstrating the effectiveness of the measures with a cost-benefit analysis.

4 WINNING CONSORTIA SU-ICT-03-2018

Cybersecurity

Horizon 2020 pilot projects

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

More than **€63.5 million** invested in **4 projects**

 <p>CONCORDIA Cyber security competence for Research and Innovation</p> <p> Partners: 46</p> <p> EU Member States involved: 14</p> <p>Key words SME & startup ecosystem Ecosystem for education Socio-economic aspects of security Virtual labs and services Threat Intelligence for Europe DDoS Clearing House for Europe AI for cybersecurity Post-Quantum cryptography</p>	 <p>Cyber Security for Europe</p> <p> Partners: 43</p> <p> EU Member States involved: 20</p> <p>Key words Cybersecurity for citizens Application cases Research Governance Cyber Range Cybersecurity certification Training in security</p>	 <p>ECH</p> <p> Partners: 30</p> <p> EU Member States involved: 15</p> <p>Key words Network of Cybersecurity centres Cyber Range Cybersecurity demonstration cases Cyber-skills Framework Cybersecurity certification Cybersecurity early warning</p>	 <p>SPARTA</p> <p> Partners: 44</p> <p> EU Member States involved: 14</p> <p>Key words Research Governance Cybersecurity skills Cybersecurity certification Community engagement International cooperation Strategic Autonomy</p>
--	---	---	---

Last updated 8 March 2019

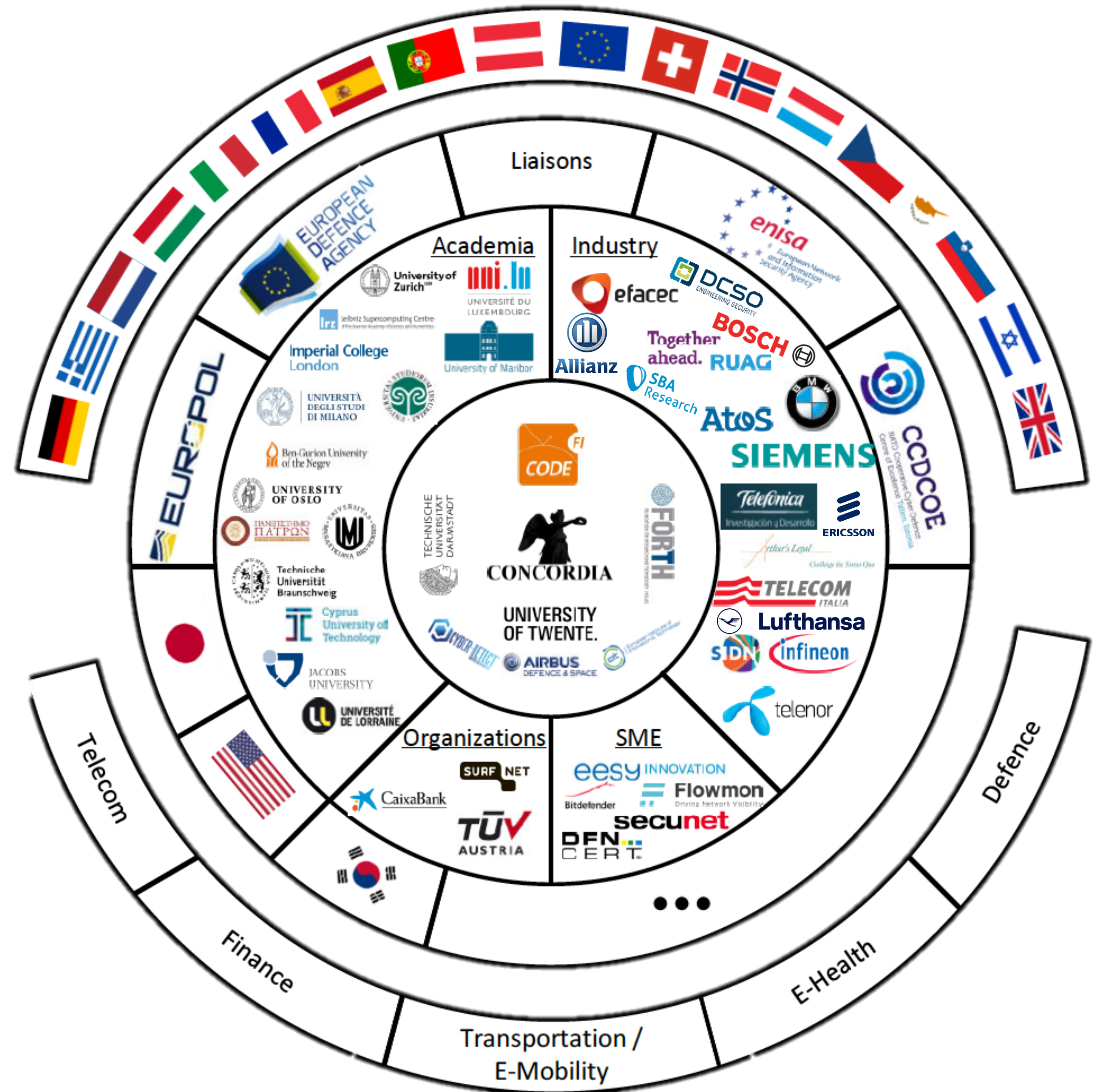
More than **160 partners** from **26 EU Member States**



BUSINESS FINLAND

55 Partners:

- 27 Academia
- 28 Industry and Organisations



- 16 Millions EC funding for 4 years
- 7 Millions additional funding from national authorities and industry

Who Are CyberSec4Europe?

Centres of Excellence /
Universities / Research
Centres / SMEs

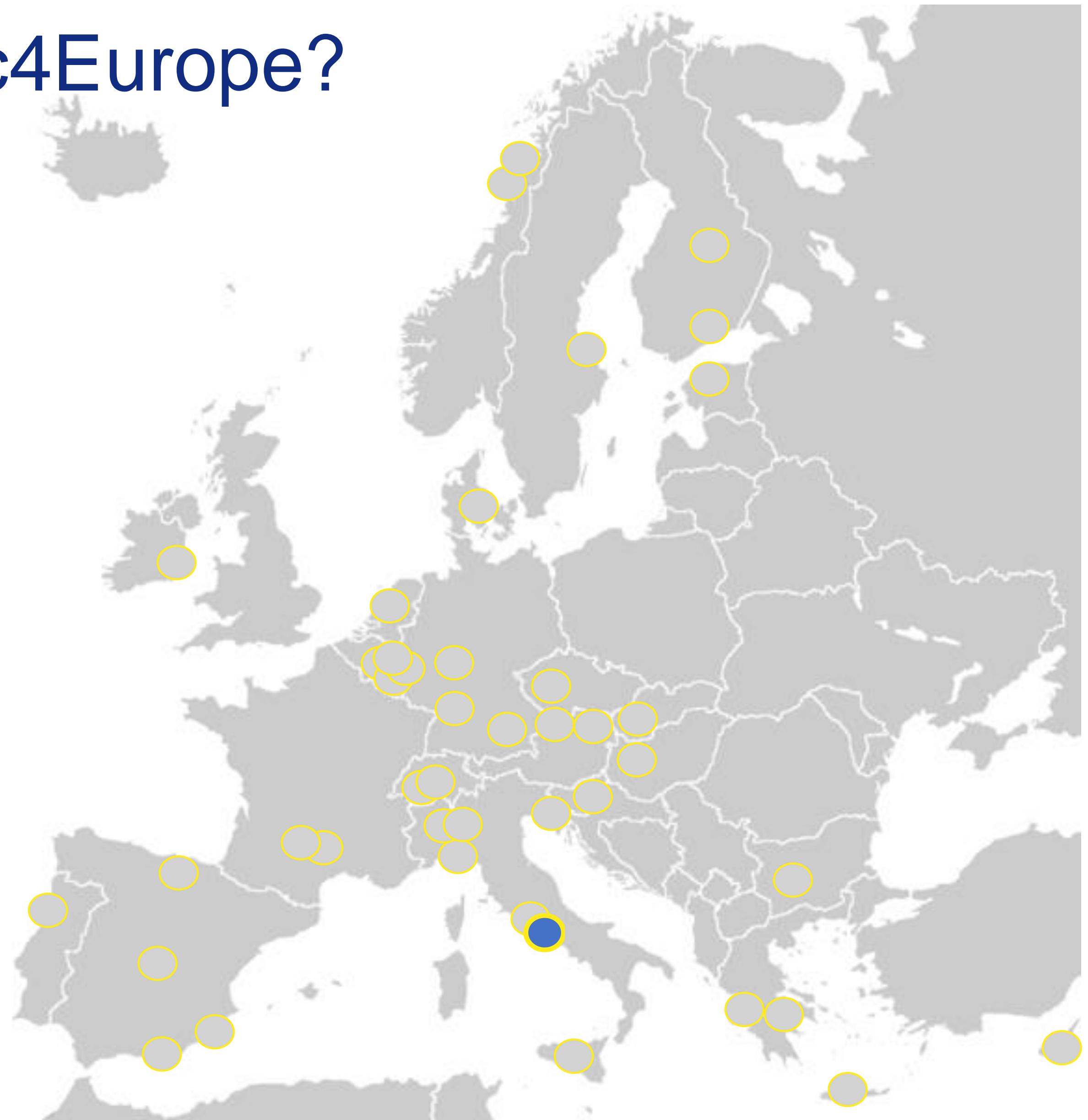
43 partners in 22 countries

26 ECOSO members
involved in 6 ECOSO
Working Groups

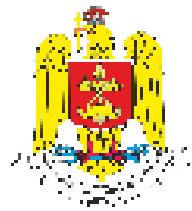
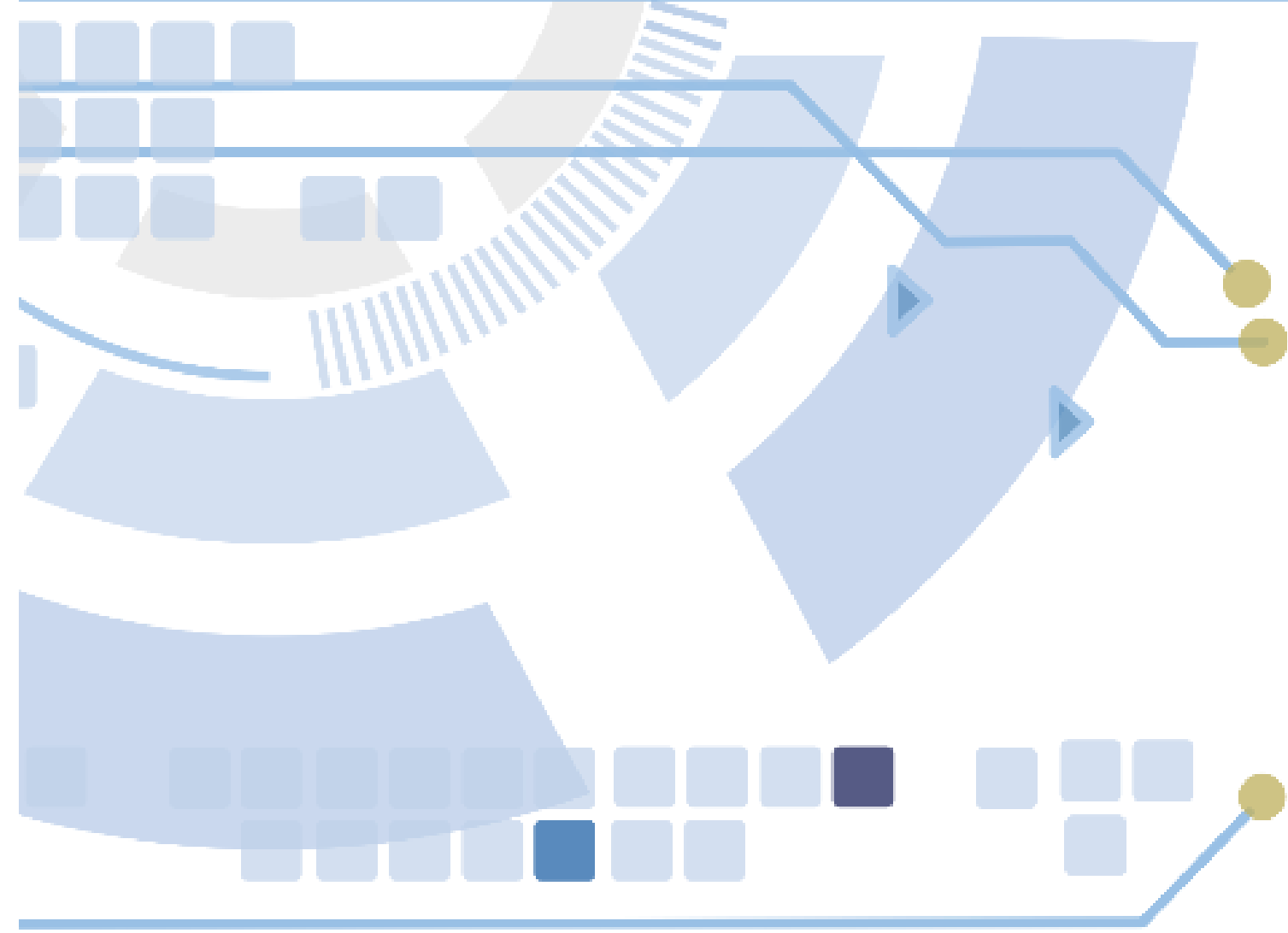
Existing networks (ECOSO,
TDL, EOS, CEPIS)

Experience from over 100
cybersecurity projects in 14
key cyber domains

11 technology/ application
elements and coverage of
nine vertical sectors



PARTNERS



University
RTO
Company / SME
Centre
Gov/Auth



EE	UTARTU
Tartu Ülikool	
University	

LV	LMT
Latvijas Mobilais Telefons	
Company	

LT	KTU
Kauno Techn. Universitetas	
University	
LT	L3CE
Liet. kibet. nauk. komp. ir tyr. centrs	
Centre	
LT	LKA
Lietuvos Karo Akademijs	
University	
LT	MRU
Mikolo Romerio Universitetas	
University	

A STRONG BASIS OF EXCELLENCE

44 partners spanning academia, industry, institutions, grassroots

Pragmatically anchored in member states

STRATEGIC PROGRAMS

Multilevel supervision

Continuous and flexible evaluation

Trustworthy intelligent infrastructures

Fair and secure AIs

THE STAKES OF EUROPEAN AUTONOMY

Design a long-term roadmap and network of competence centers

PT	INOV
INOV	
RTO	
PT	IST
Instituto Superior Técnico	
University	

ES	EUT
Eurecat	
RTO	
ES	TEC
Tecnalia	
RTO	

ES	INDRA
Indra	
Company	
ES	VICOM
Vicomtech	
RTO	

IT	CINI
Cons. Interuniv. Naz. per l'Informat.	
University	
IT	CNR
Consiglio Naz. delle Ricerche	
RTO	

IT	CNIT
Cons. Naz. Interuniv. Telecom.	
University	
IT	ISCOM
Ist. Sup. del Com. e del Techn.	
Gov/Auth	

IT	LEO
Leonardo	
Company	

FR	CEA
Commissariat à l'Énergie Atomique	
RTO	
FR	INRIA
Inria	
RTO	

FR	ANSSI
Agence Nationale de la SSI	
Gov/Auth	
FR	TCS
Thales	
Company	

FR	IMT
Institut Mines Telecom	
University	
FR	YWH
Yes We Hack	
Company	

BE	CETIC
Centre d'Excel. en TIC	
RTO	
BE	UNAM
Université de Namur	
University	

LU	LIST
Luxemb. Inst. of Science and Tech.	
RTO	
LU	SML
Securitymadein.lu	
Gov/Auth	

LU	UNI
Université du Luxembourg	
University	

DE	FTS
fortise	
RTO	
DE	SAP
SAP Software Solutions	
Company	

DE	UBO
Universität Bonn	
University	

DE	FHG
Fraunhofer (FS)	
RTO	
DE	TUM
Technische Univ. München	
University	

DE	UKON
Universität Konstanz	
University	

PL	ITTI
ITTI	
SME	

PL	NASK
Naukowa i Akad. Sieć Komputerowa	
RTO	

PL	PPBW
Polska Platforma Bezp. Wzrost.	
Centre	

CZ	CESNET
CESNET	
RTO	

CZ	BUT
Vysoké Učení Technické v Brně	
University	

CZ	NIC
CZ.NIC	
Gov/Auth	

AT	JR
Joanneum Research	
RTO	

AT	TNK
Technikon	
SME	

EL	KMR
Κέντρο Μελετών Ασφάλειας	
Gov/Auth	

EL	NCSR
Demokritos	
RTO	



WHAT & WHO & WHERE?

Contacts to Consortia & ECSO

- ✓ CONCORDIA: *Antonio Ken Iannillo*, SnT, LU, antonioken.iannillo@uni.lu & *Olivier Festo*, INRIA, FR olivier.festor@inria.fr
- ✓ CyberSec4Europe: *David Goodman*, Trust in Digital Life, UK, david@trustindigitallife.eu
- ✓ ECHO: *Matteo Merialdo*, RHEA GROUPO, BE, m.merialdo@rheagroup.com
- ✓ SPARTA: *Géraud Canet*, CEA, FR, geraud.canet@cea.fr
- ✓ ECSO: *Roberto Cascella*, roberto.cascella@ecs-org.eu

What Else to Do?

- ✓ Join: [Business Finland | Horizon 2020 Group in LinkedIn](#)
- ✓ Subscribe: [Business Finland | Newsletter](#)
- ✓ Visit: [Business Finland | Digital Trust Finland Program](#)
- ✓ Check: [Finnish Horizon 2020 Contacts & Organizations](#)
- ✓ Explore: [Finnish Information Security Cluster - FISC ry](#)

Key Platforms (cPPPs, 1/2)

- Factories of the Future (<http://www.effra.eu>)
- Energy-efficient Buildings (<http://e2b.ectp.org>)
- European Green Vehicles Initiative (<http://www.egvi.eu>)
- Sustainable Process Industry (<https://www.spire2030.eu>)
- Photonics (<http://www.photonics21.org>)
- Robotics (<https://eu-robotics.net>)

Key Platforms (cPPPs, 2/2)

- High Performance Computing (<http://www.etp4hpc.eu>)
- Advanced 5G networks for the Future Internet (<https://5g-ppp.eu>)
- Big Data (<http://www.bdva.eu>)
- ECSO (<https://www.ecs-org.eu>) + FISC (<http://www.fisc.fi>)
- AIOTI - Alliance Internet of Things Innovation (<https://aioti.eu>)



APPENDIX

KEY EVENTS - 2H/2019

Key ICT Event Dates [Finnish Presidency]

[EUROPEAN BIG DATA VALUE FORUM 2019 \(14 – 16 Oct\)](#)

The European Big Data Value Forum is a key European event for industry professionals, business developers, researchers, and policy makers to discuss the challenges and opportunities of the European data economy and data-driven innovation in Europe. About 700 attendees expected, event is coordinated by VTT.

Key ICT Event Dates [Finnish Presidency]

SECURITY RESEARCH EVENT 2019 (6 – 7 Nov)

SRE 2018 will gather 800 participants representing a wide range of security stakeholders: researchers, industry representatives, public security providers and practitioners (for example fire departments, police forces and border guard and law enforcement agencies), as well as policymakers.

SET-Plan (14 – 15 Nov)

SET Plan conference 14. – 15.11.2019 targets to energy sector for about 500 participants.

Key ICT Event Dates [Finnish Presidency]

[EF ECS - European Forum for Electronic Components and Systems \(19 – 21 Nov\)](#)

EF ECS 19. – 21.11.2019 is the international forum with a focus on 'Our Digital Future' along the Electronic Components and Systems value chain in Europe. The organizers of the event include ECSEL Joint Undertaking and the European Commission, in association with EUREKA. Around 700 participants are expected.



APPENDIX

NCP@YOUR SERVICE

What an NCP Can Do 4 You? (1)

- ✓ To inform and to provide general and specific info about calls, conditions and offer Commission's annotated info.
- ✓ To assist, advise and train e.g. about project submission, budgeting and reporting. Offers project pre-proposal check & pitching coaching.
- ✓ All difficult questions are welcome since NCP has direct contacts to solve them from European Commission.
- ✓ Signposting and cooperation with other funding opportunities (national & international).

What an NCP Can Do 4 You? (2)

- ✓ Finnish NCPs act as a co-delegate and expert members in different theme focused committees (e.g. ICT, Health, Security) in order to provide hints where EC R&D&I activities, funding instruments and conditions are evolving.
- ✓ Business Finland has close cooperation nationally between Academy of Finland, VTT, Sitra, different ministries and key stakeholders to affect e.g. Finnish proposal bilateral discussions with Commission and to join forces with other delegates/NCPs.

What an NCP Can Do 4 You? (3)

- ✓ Possibility to use national voice to foster Finnish research and innovation in the short term & in the long run (2021-2027).
- ✓ NCP can provide call statistics, conclusions and reasons behind success rates. NCP has the access to all proposal Evaluation Summary Reports which provide valuable information about different consortia and lessons to learn.
- ✓ Business Finland NCPs have the access to Business Finland customer portfolio (research and corporate projects) which helps to build either domestic and international consortia.

What an NCP Can Do 4 You? (4)

- ✓ NCPs at the Academy of Finland are running the competed national research funding calls and this gives a synergetic value for advising the R&I field with the EU calls as well.
- ✓ Business Finland has close cooperation between e.g. Sweden, Norway and Japan which helps to organize other type of international R&D funding not linked to European Commission.
- ✓ Knows about the key technology platforms, PPPs and events in EU in advance.
- ✓ Last but not least: no conflicts of interest.

WORLD IDEAS

Pauli Stigell

Expert, National Contact Point

+358 50 557 7856

pauli.stigell@businessfinland.fi

Pekka Rantala

Expert, National Contact Point

+358 50 396 2922

pekka.rantala@businessfinland.fi