



General Matters

Call 2019





POLICY CONTEXT

Security Union

A Europe that protects



04/2015: European Agenda on Security defines the priority actions at EU level to ensure an effective EU response to security threats over the period 2015-2020

"Research and innovation is essential if the EU is to keep up-to-date with evolving security needs. Research can identify new security threats and their impacts on European societies. It also contributes to creating social trust in research-based new security policies and tools. Innovative solutions will help to mitigate security risks more effectively by drawing on knowledge, research and technology."

10/2016: new Commissioner for the Security Union, supported by a horizontal Task Force involving 30 different services in the commission and the EEAS

Mission letter of Julian King as Commissioner for Security Union:

"During our mandate, I would like you to support the Commissioner for Migration, Home Affairs and Citizenship in the following tasks:

*[...] "Ensuring that EU-financed **security research** targets the **needs of security practitioners** and develops solutions to forthcoming security **challenges** [...]."*

12/2018 Seventeenth Progress Report towards an effective and genuine Security Union

Section on EU Security Research

“EU security research is one of the building blocks of the Security Union enabling innovation in technologies and knowledge crucial for developing capabilities to address today's security challenges, anticipating tomorrow's threats and contributing to a more competitive European security industry.”

*“Given the particular nature of the security sector (in which the market is represented mainly by public authorities), appropriate **uptake of research output** can be guaranteed only if research is acknowledged as one of the building blocks of a wider **capability development process** bringing together policy-makers, practitioners, industry and academia. The **close involvement of all stakeholders** at an early stage is instrumental to identify capability gaps, and define capability priorities that can, when needed, trigger research requirements.”*

The Challenge

The security research landscape

Notwithstanding the effort still **gap between research output and market uptake**

- highly fragmented and mostly institutional market
- the limits of existing funding schemes
- the misalignment between demand and supply

Budgetary Overview

Topics (Type of Action)	Budgets (EUR million)			Deadlines
	2018	2019	2020	
Opening: 15 Mar 2018				
SU-GM01-2018-2019-2020 (CSA)	5,0			28-Aug-18
SU-GM02-2018-2020 (CSA)	6,0			
SU-GM03-2018-2019-2020 (PCP)	9,7			
Opening: 19 Mar		2019		
SU-GM01-2018-2019-2020 (CSA)		3,5		22-Aug-19
SU-GM03-2018-2019-2020 (PCP)		-		
Opening: TBD				
Focus area topic(s) for 2020			2020	
			TBD	To be defined
Overall indicative budget	20,7	3,5		

Research is not a stand-alone process

Research is part of a wider process:

The Capability Development Process

Networks of Practitioners

EC objective: To address difficulties for the uptake of research results

The **Networks of Practitioners** will play a relevant role in supporting the Security Capability Development Cycle as per being devoted to:

- Find common needs and capability gaps in the security domain
- express common user/functional requirements for innovative solutions addressing the 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 or the industrialization of research results
- indicate priorities as regards domains requiring more standardization

Networks of Practitioners

The four (+1) pillars of NoP:

- The networks is “out there”. The projects should act as network enablers.
 - **NETWORKING**
- The networks of practitioners are not just another research and innovation project. The networks of practitioners are expected to catalogue, aggregate, process and disseminate the existing knowledge on their respective areas of interest (meta- research).
 - **(META) RESEARCH**
 - **DEMONSTRATION**
- The networks of practitioners should deliver periodic findings (each 6 months or less) on the three main goals in a flexible and reactive way.
 - **COMMUNICATION**

Networks of Practitioners

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)

 **+ 2 new (2018 call)**

SU-GM01-2018-2019-2020

Pan-European networks of practitioners and other actors in the field of security

a. **[2019-2020] Practitioners (end-users) in the same discipline and from across Europe** are invited to get together:

- 1) to monitor research and innovation projects with a view to recommending the uptake or the industrialisation of results
- 2) to express common requirements as regards innovations that could fill capability and other gaps and improve their future performance, and
- 3) to indicate priorities as regards areas requiring more standardisation.

- **Areas of specialization:**

- ~~Protection of public figures (CANCELLED)~~
- Handling of hybrid threats

- **Type of action:** Coordination and Support Action

- **Estimated EU contribution:** EUR 3,5M

- **Recommended duration:** 5 years

Policy Context (encore)

JOIN(2016) 18 final - Joint Framework on countering hybrid threats

- Joint framework with actionable proposals to help counter hybrid threats.
- Cross-border dimension can be addressed more effectively at EU level
- Facilitate a holistic approach that will enable the EU, in coordination with MS
- Build on existing strategies and sectoral policies (e.g. security, defence, cybersecurity, energy, maritime, CIP, transport, supply chain, space...)

EC Press release – 13/06/2018

- Further steps in response to hybrid and CBRNE threats.
- Hybrid activities by state and non-state actors continue to pose a serious and acute threat to the EU and its Member States.

COM(2018) 470 final - Security Union Progress Report #15

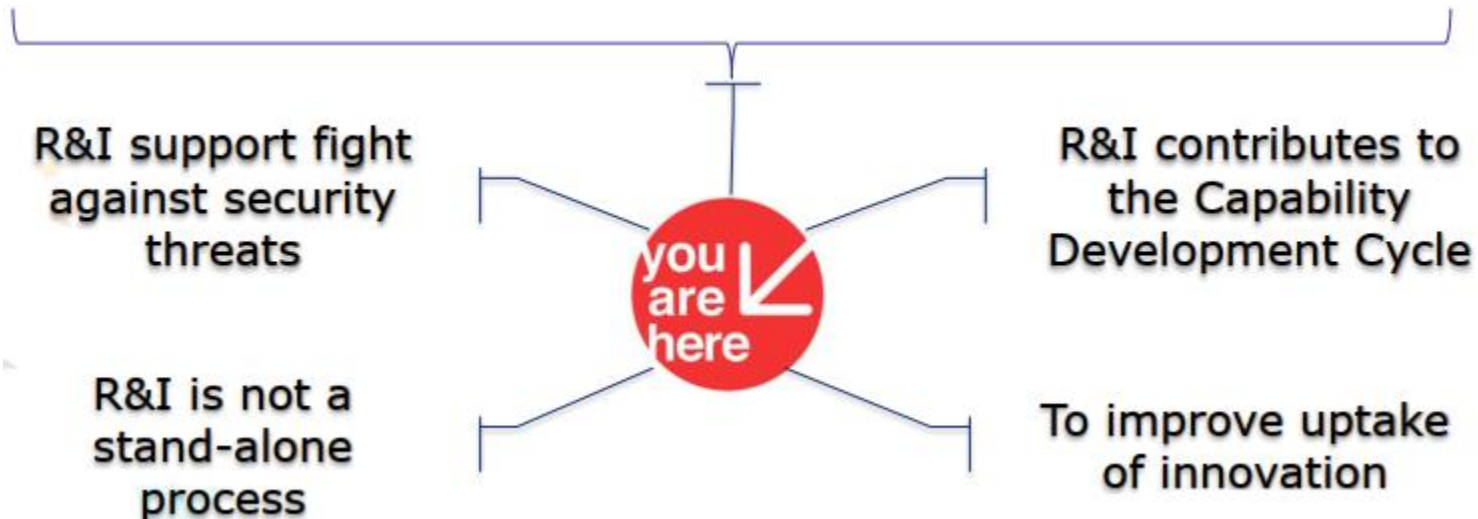
- Joint Communication on Increasing resilience and bolstering capabilities to address hybrid threats;
- Joint Report on the implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018

Policy Context (encore)

JOIN(2018) 16 final - Increasing resilience and bolstering capabilities to address hybrid threats

Identify areas where action should be intensified:

- Situational awareness – improved capacity to detect hybrid threats
- Reinforced actions against Chemical, Biological, Radiological and Nuclear threats
- Strategic communication – coherent dissemination of information
- Building resilience and deterrence in the cybersecurity sector
- Building resilience to hostile intelligence activity



Eligibility criteria

- **For part a):** Practitioner participation from at least 8 Member States or Associated Countries is mandatory.
- Each proposal must include a plan, and a budget amounting at least **25% of the total cost of the action to interact** with industry and academia and other providers outside the consortium with a view to assessing the feasibility of their findings.
- Each consortium must commit to produce, **every 6 or fewer months, a report about their findings** in the 3 lines of action (see in “Scope”);
- Each proposal must include a work-package to **disseminate their findings**, including an **annual workshop or conference**.



Thank you!

#InvestEUresearch

www.ec.europa.eu/research

Participant Portal www

<http://ec.europa.eu/programmes/horizon2020/en/h2020-section/cross-cutting-activities-focus-areas>