Horizon 2020 Security

THE FIC 2018 PITCHING SESSION

Introduction

Lille, January 24th 2018

Armand Nachef, CEA, NCP Security - France

Political background to Horizon 2020

The Treaties

- The Eu Coal and Steel Community in 1951
- The Eu Atomic Energy Community in 1957
- … the single act in 1986 in EEC treaty for research policy
- The Lisbon Treaty 2007: Article 179 - ERA

The European Union institutions prepare Policies

- Research and Innovation Policy
- Regional Policy
- Education Policy
- …

Funding

- Horizon 2020
- European Structural and Investment Funds
- Erasmus Plus
- …

Framework Programmes
for Research and Technological Development

- Created by the European Union to support and foster research in the European Research Area
- Work programmes are defined by the Commission aided by official advisory groups and lobby groups
- Steadily increasing budget
- From FP1 to FP 7, the focus was in technological research
- Focus in H2020 is in Innovation

Framework Programme	Period	Budget (Billion €)
FP 1	1984-1987	3.8
FP 2	1987-1991	5.4
FP 3	1990-1994	6.6
FP 4	1994-1998	13.2
FP 5	1998-2002	15.0
FP 6	2002-2006	17.9
FP 7	2007-2013	50.5
Horizon 2020 (FP8)	2014-2020	77

The participation process

1. The European Commission publishes the work programme

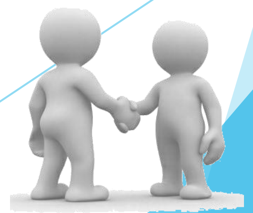
2. You need to find a relevant topic in this work programme

3. Then you need to find partner(s) for your project to integrate or to form a consortium in order to co-write the proposal responding to all the requirements of the topic
   - ✓ Sell yourself, provide ideas not just technology
   - ✓ Work hard during the proposal preparation
   - ✓ Understand your role and match it to the budget

4. The consortium coordinator submits the proposal before deadline
5. You wait for the evaluation to take place

... in case of positive evaluation...

6. You sign the Grant Agreement and start implementing your project



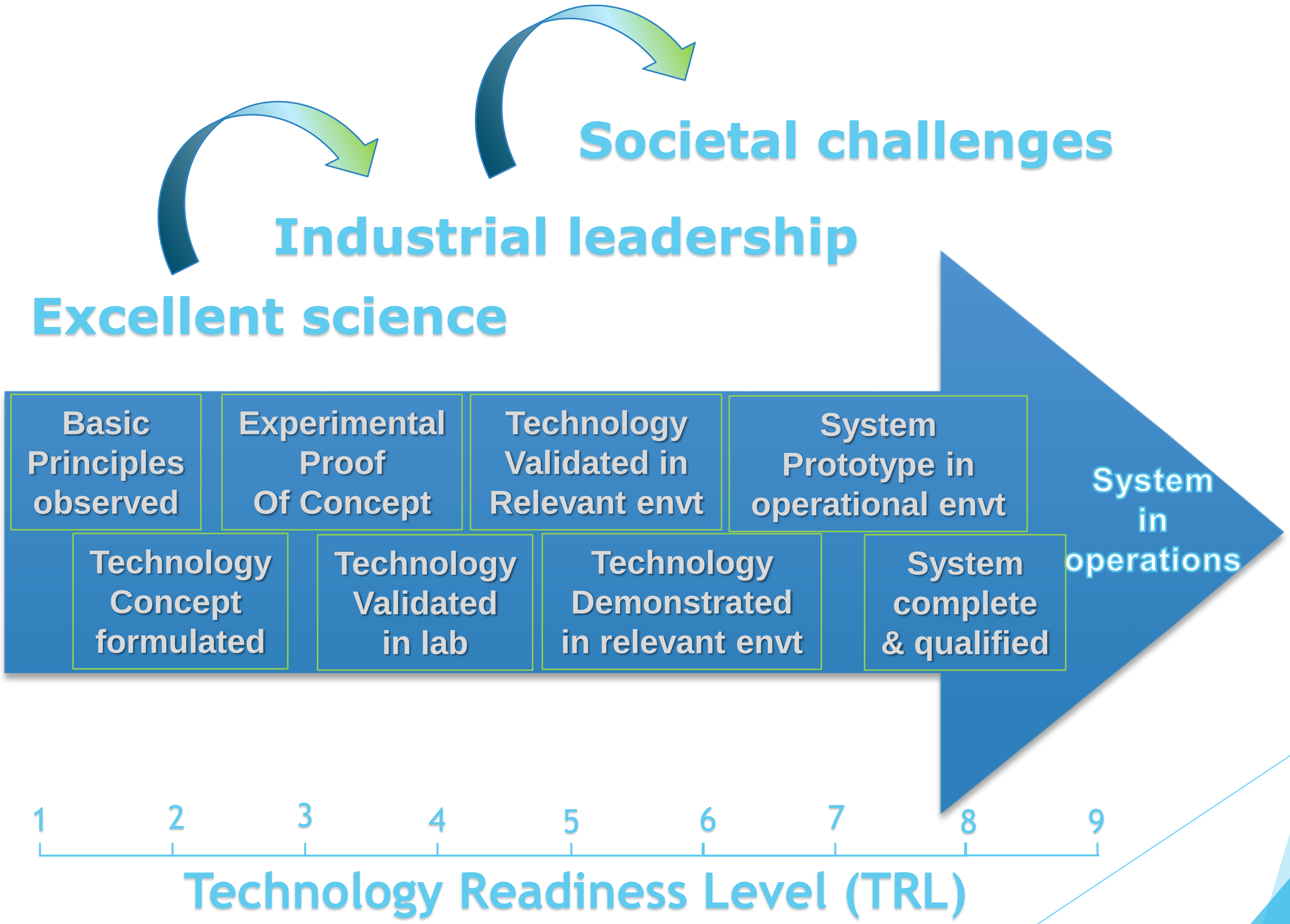
Who can participate?

- Industry – Multinationals to SMEs
- Research organisations
- Universities & other HEIs
- Public bodies, for example
  1. firefighters,
  2. police and intelligence communities,
  3. border guards,
  4. custom authorities,
  5. explosive specialists,
  6. forensic laboratories,
  7. medical emergency teams
  8. other practitioner disciplines
- Trade Associations
- International bodies

Why participate in Horizon 2020?

- Tackling global challenges together
  - challenges that affect us all, such as infectious diseases, security, or climate change, can only be solved at international level
- Funding for excellent science
- Focus on innovation
  - encourages innovators to move their ideas from the lab to the market
- World-class research infrastructures
  - facilitates the continued development of global research infrastructures, ensuring global interoperability and access
- Access to new networks and alliances
  - raising the profile of your research in an international project, sharing expertise and access to equipment, data and facilities
- Excellent rate of funding
  - Up to 100% of total eligible costs
  - Limited to maximum 70 % for actions close to market except for non-profit institutions who will be able to receive up to 100%
  - For indirect costs, a flat rate of 25 % of the direct eligible costs is applied

Coverage of the full innovation chain



Societal challenges

Industrial leadership

Excellent science

Basic Principles observed

Technology Concept formulated

Experimental Proof Of Concept

Technology Validated in lab

Technology Validated in Relevant envt

Technology Demonstrated in relevant envt

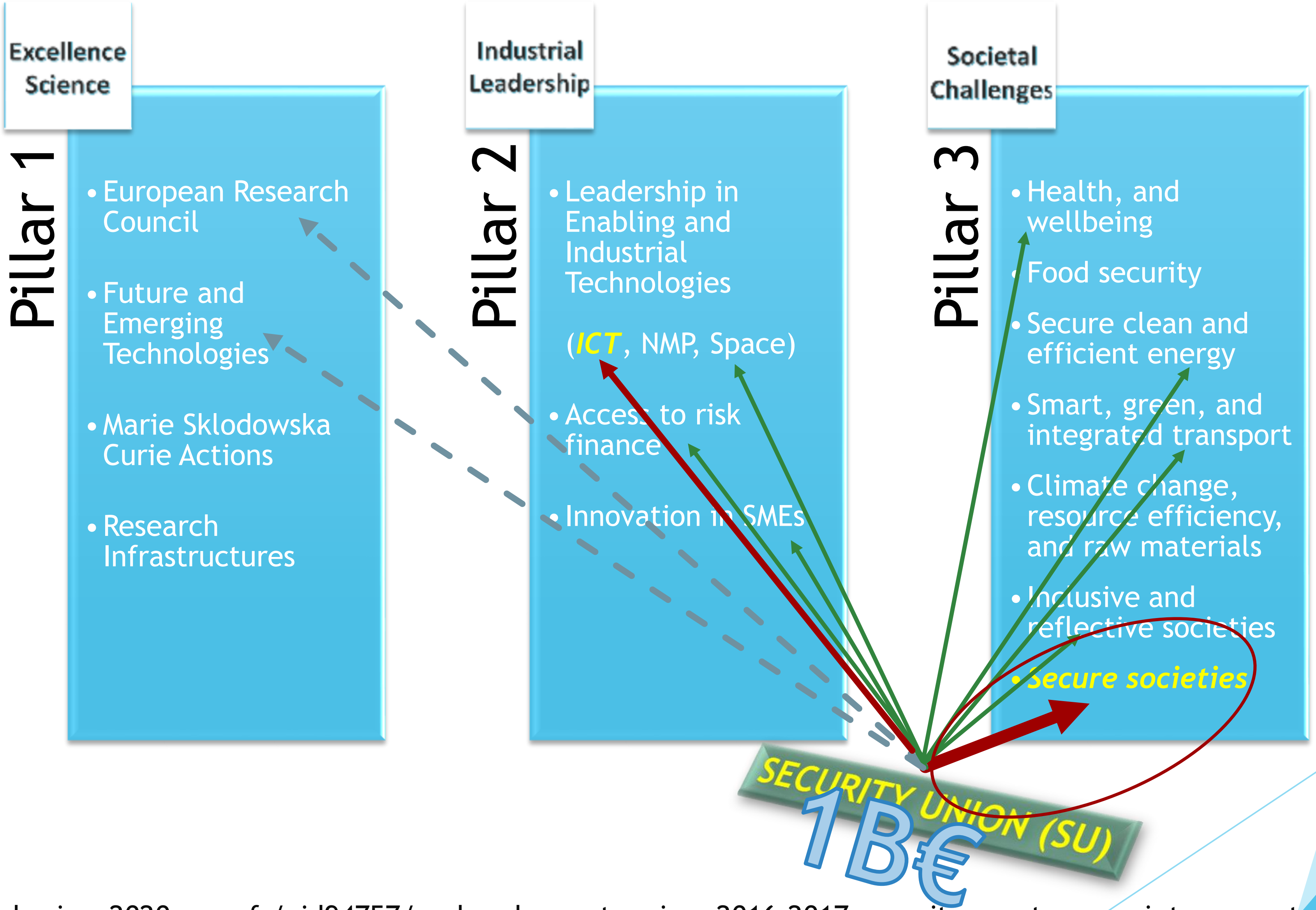
System Prototype in operational envt

System complete & qualified

System in operations

Technology Readiness Level (TRL)

The “Security Union” focus area in Horizon 2020



Pillar 1

Excellence Science

- European Research Council
- Future and Emerging Technologies
- Marie Sklodowska Curie Actions
- Research Infrastructures

Pillar 2

Industrial Leadership

- Leadership in Enabling and Industrial Technologies

  (*ICT*, NMP, Space)
- Access to risk finance
- Innovation in SMEs

Pillar 3

Societal Challenges

- Health, and wellbeing
- Food security
- Secure clean and efficient energy
- Smart, green, and integrated transport
- Climate change, resource efficiency, and raw materials
- Inclusive and reflective societies
- ***Secure societies***

http://www.horizon2020.gouv.fr/cid94757/recherche-partenaires-2016-2017-securite-montage-projets-competences-demandees-offertes.html

http://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-security_en.pdf

Call for proposals – 2018-2019-2020

SU-INFRA

Physical and cyber threats to critical infrastructure
INFRA01 (IA)

Security for Smart Cities and "soft" targets in Smart Cities
INFRA02 (IA)

SU-DRS

Human factors for DRS
DRS01(RIA)

Technologies for first responders
DRS02 (RIA)

Pre-normative R&Demo for DRS
DRS03 (IA)

CBRN cluster
DRS04 (RIA)

Management of pandemic crises
DRS05 (IA)

SU-FCT

Human factors to FCT
FCT01 (RIA)

Technologies to FCT
FCT02 (RIA)

Information and data stream Mgt
FCT03 (IA)

Explosives
FCT04 (IA)

SU-BES

Human factors for BES
BES01 (RIA)

Technologies for BES
BES02 (RIA)

Demo of applied solutions
BES03 (IA)

SU-GM

Networks of practitioners
GM01 (CSA)

PCP of advanced Systems
GM02 (CSA) (PCP)

PCP of Solutions
GM03 (PCP)

SU-DS

Cybersecurity preparedness
DS01 (IA)

Management of cyber-attacks
DS02 (IA)

Privacy for SMEs and citizens
DS03 (IA)

Electrical Syst.
DS04 (IA)

accountability in critical sectors
DS05 (RIA) (IA)

SU-ICT

Dynamic countering
ICT01 (IA)

Building blocks for resilience
ICT02

Cybersecurity Competence Network
ICT03 NEW 2018

Quantum Key Distribution testbed
ICT04 (IA) 2018

Link with ICT

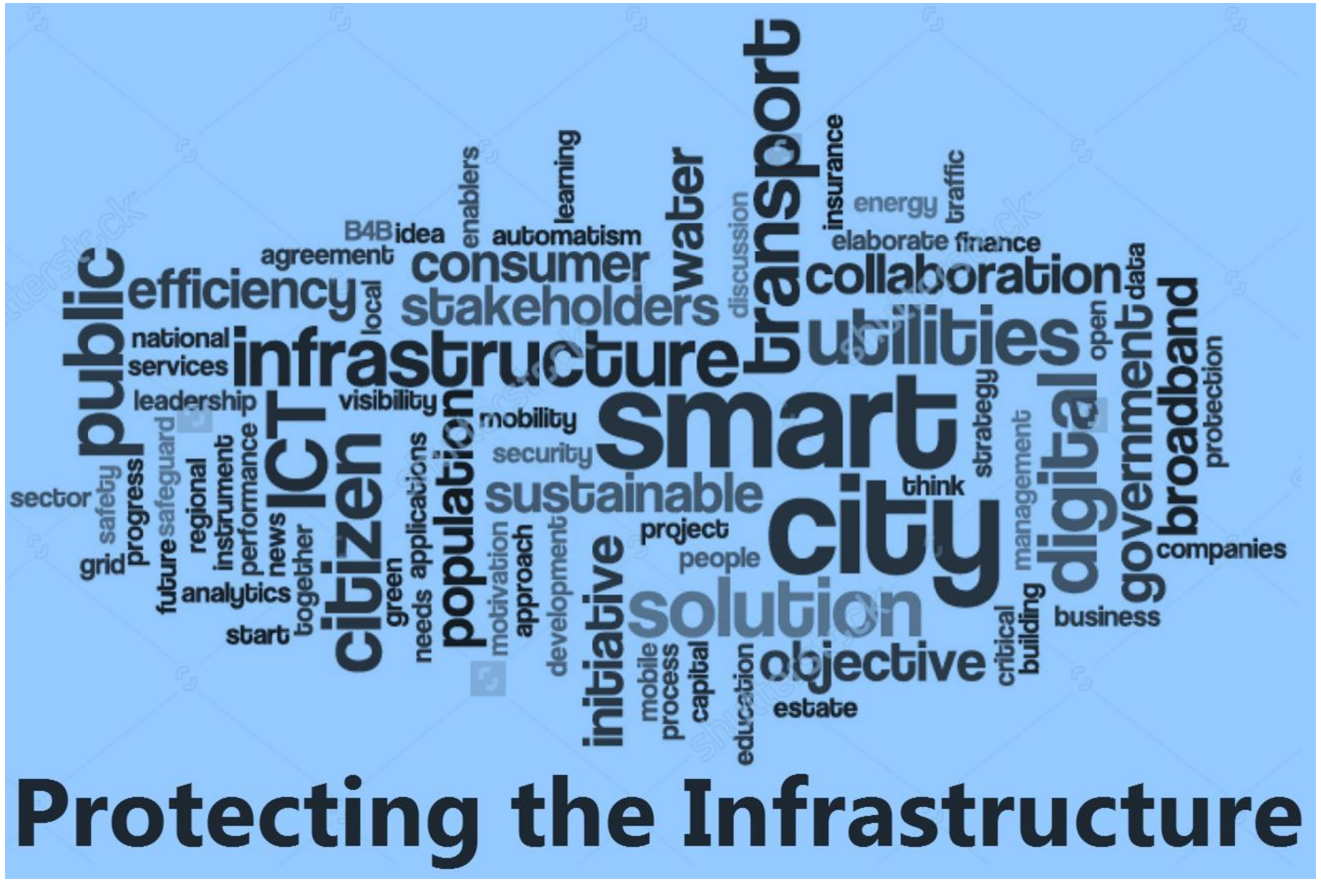
NEXT BROKERAGE EVENT

- 1st & 2nd February 2018, The Security Mission Information & Innovation Group (SMI2G) event
  http://www.imgs-eu.org/home/public-documents/save-the-dateforthesmi2gmeeting2018

APPENDIX

SU-INFRA

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



Protecting the Infrastructure

Call – SU-INFRA

Mission:

The aim is to protect and improve the resilience of critical infrastructures, supply chains and transport modes.

2 topics

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

2. SU-INFRA02-2019:
   Security for Smart Cities and "soft" targets in Smart Cities

SU-INFRA : 2018 → 2020

Year	Topic (Type of Action)	Title	Budget (M€)	Deadline
2018	SU-INFRA01-2018-2019-2020 (IA)	Combined physical and cyber threats	24,0	23 Aug 2018
2019	SU-INFRA01-2018-2019-2020 (IA) SU-INFRA02-2019 (IA)	Combined physical and cyber threats “Soft" targets in Smart Cities	22,0 16,0	22 Aug 2019
2020	SU-INFRA01-2018-2019-2020 (IA)	Combined physical and cyber threats	18,0	27 Aug 2020

SU-INFRA01-2018-2019-2020 * (1/2)

Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe

Type of Action	Innovation Action
Output TRL	7
Project duration	maximum **24 months**
Budget per project	between 7 and 8 M€
Total budget	24 M€ in 2018 ------ 22 M€ in 2019 ------ 18 M€ in 2020
Eligibility conditions	At least 2 operators as beneficiaries (not necessary coordinators) Participation of industry to provide security solutions *Consortia should involve, infrastructure owners and operators, first responders, industry, technologists, social scientists, and SMEs.*
Deadline	23 Aug 2018 ------ 22 Aug 2019 ------ 27 Aug 2020

- **Challenge**
  - ❑ Increased combined physical and cyber-attacks due to their interdependencies.
  - ❑ Need of a **complete approach to secure** existing or future connected and interdependent **installations, plants and systems**.
  - ❑ New security solutions need to be more cost-effective and automated.

SU-INFRA01-2018-2019-2020 - Scope (2/2)

Forecast, assess physical and cyber risks, prevent, detect, response, mitigate consequences, and achieve fast recovery (including novel installation designs)

Achieve the security and resilience of all functions performed by the installations, and of neighbouring populations and the environment.

Share information with the public in the vicinity of the installations (including through social media and with the involvement of civil society organisations), for ensuring service continuity and for the protection of first responders such as rescue teams, security teams and monitoring teams.

Proposals should:

a) address all aspects of interdependent
- physical threats and incidents (e.g. bombing, sabotage and attacks with a variety of weapons against installations, plane or drone overflights and crashes, spreading of fires, floods, landslides, disastrous consequences of global warming, seismic activity, space weather, combined threats, etc.)
- cyber threats and incidents (e.g. malfunction of SCADA system, non-authorised access of server, electronic interference, distributed attacks),
- the cascading risks resulting from such complex threats,

b) demonstrate the accuracy of their risk assessment approach using specific examples and scenarios of real life

c) enhance real-time security management of physical and cyber threats, taking account of the ageing of existing infrastructure.

One of the following critical infrastructures:

- 1) water systems,
- 2) energy infrastructure (power plants and distribution, oil rigs),
- 3) transport infrastructure (airports, ports, railways, urban multimodal nodes),
- 4) communication infrastructures and ground segments of space systems,
- 5) health services,
- 6) financial services;
- 7) e-commerce and the postal infrastructure,
- 8) sensitive industrial sites and plants

Proposals similar to projects financed in the previous years since 2016, won’t be selected.

SU-INFRA02-2019 (1/2)

Security for Smart Cities and "soft" targets in Smart Cities

Type of Action	Innovation Action
Output TRL	7
Project duration	maximum **24 months**
Budget per project	~8 M€
Total budget	16 M€ in 2019
Eligibility conditions	At least 2 cities or metropolitan areas as beneficiaries Participation of industry to provide security solutions
Deadline	22 August 2019

- **Challenge**
    - Open areas in cities constitute “soft targets”, that are subject to “low cost” attacks impacting all citizens.
        - Sharing big data in smart cities make urban services more responsive, and able to act upon real-time data
        - Leveraging networks of detection and prevention capabilities to enhance first responders' actions
    - The distinct smart technological and communication environments (urban, transport infrastructures, companies, industry) within a smart city require a common cybersecurity management approach.

SU-INFRA02-2019 Scope (2/2)

- Develop and integrate experimentally, in situ, the components of an **open platform for sharing** and managing information between public service operators and security practitioners of a large, smart city.
- involve actively the security actors of the city area, their coordination and governance;
- Ensure the interconnection of the city smart systems with the systems of the security practitioners;
- Address at least one of the following key issues:
  A. Simulation, detection and analysis of the security threats and risks of the interconnection of smart systems
  B. Delivery of a cyber-security framework to ease collaboration across all smart cities stakeholders;
  C. Support and implementation of a common approach to securing and managing the data.
- Consider how to combine, inter alia:
  - Methods to detect weapons, explosives, toxic substances
  - Systems for video surveillance
  - Methods to identify, and neutralize crime perpetrators whilst minimizing intrusion into crowded areas
- Enhance the security of city smart systems: access control, secure communication and data storage;
- Consider mitigation strategies to increase resilience;
- Integrate modules to simulate security incidents, and their consequences;
- Integrate modules to measure the quantitative and qualitative impact of the platform on security;
- Provide tools for the sharing, consolidation and analysis of multi-sourced data.
- Integrate digital security awareness into the eco-system of humans, competences, services and solutions.

SU-DRS

Disaster-Resilient Societies

Call – SU-DRS

Mission:

The aim is to advance innovation in the society at large, and among first responders, to reduce the loss of human life and to reduce environmental, economic and material damage from natural and man-made disasters, including from climate-related weather events, earthquakes and volcanic events, space weather events, industrial disasters, crime and terrorism threats.

5 topics

1. SU-DRS01-2018-2019-2020:
   Human factors, and social, societal, and organisational aspects for disaster-resilient societies
2. SU-DRS02-2018-2019-2020:
   Technologies for first responders
3. SU-DRS03-2018-2019-2020:
   Pre-normative research and demonstration for disaster-resilient societies
4. SU-DRS04-2019-2020:
   Chemical, biological, radiological and nuclear (CBRN) cluster
5. SU-DRS05-2019:
   Methodical demonstration of novel concepts for the management of pandemic crises

SU-DRS : 2018 → 2020

Year	Topic (Type of Action)	Title	Budget (M€)	Deadline
2018	SU-DRS01-2018-2019-2020 (RIA)	Human factors for DRS	5,0	23 Aug 2018
	SU-DRS02-2018-2019-2020 (RIA)	Technologies for first responders	21,0	
	SU-DRS03-2018-2019-2020 (IA)	Pre-normative R&Demo for DRS	6,0	
2019	SU-DRS01-2018-2019-2020 (RIA)	Human factors for DRS	5,0	22 Aug 2019
	SU-DRS02-2018-2019-2020 (RIA)	Technologies for first responders	21,0	
	SU-DRS03-2018-2019-2020 (IA)	Pre-normative R&Demo for DRS	6,0	
	SU-DRS04-2019-2020 (RIA)	CBRN cluster	10,5	
	SU-DRS05-2019 (IA)	Management of pandemic crises	10,0	
2020	SU-DRS01-2018-2019-2020 (RIA)	Human factors for DRS	TBD	27 Aug 2020
	SU-DRS02-2018-2019-2020 (RIA)	Technologies for first responders		
	SU-DRS03-2018-2019-2020 (IA)	Pre-normative R&Demo for DRS		
	SU-DRS04-2019-2020 (RIA)	CBRN cluster		

SU-DRS01-2018-2019-2020 (1/2)

Human factors, and social, societal, and organisational aspects for disaster-resilient societies

Type of Action	Research & Innovation Action
Output TRL	not specified
Project duration	not specified
Budget per project	5 M€
Total budget	5 M€ in 2018 ------ 5 M€ in 2019 ------ 5 M€ in 2020
Eligibility conditions	At least 3 first responders from 3 different EU or associated countries
Deadline	23 Aug 2018 ------ 22 Aug 2019 ------ 27 Aug 2020

- **Challenge**
  - ❑ The resilience of societies heavily on how their citizens behave individually or collectively
  - ❑ The spread of new technologies and media are inducing dramatic changes in how individuals and communities behave
  - ❑ Building the resilience requires a better understanding and implementation of these new technologies to raise disaster risk awareness, to improve citizen understanding of risks, and to enhance governance

SU-DRS01-2018-2019-2020 - Scope (2/2)

Human factors … for DRS

- Diversity in risk perception and in understanding responses to crises requires research that addresses the issues of geographical diversity (within Europe)
- Take into account cultural changes. Encompass
  - prevention (education, risk awareness) and preparedness (knowing how to react),
  - emergency management (communication before and during an event),
  - response (empowering citizens to act by themselves according to more effective practices and following established guidelines),
  - recovery
- Consider social media and crowd-sourced data, and the involvement of the citizens in the process validation
- Analyse both the positive and negative roles of social media and crowd-sourced data in crisis situations. Assess such practices for different disaster scenarios (natural hazards, industrial disasters, terrorist threats).
- Civil society organisations, first responders, (national, regional, local, and city) authorities are invited to
  - propose strategies, processes, and methods (from research results)
  - test with citizens and communities representative of European diversity, for different types of disaster
- Look into how to implement the concept of ‘Building Back Better’ of the Sendai Framework, taking account of tangible and intangible cultural heritage, and traditional know-how.
- Learn from countries are constantly under natural threat where risk is perceived differently (e.g. Japan)
- International cooperation, in particular with Japan is encouraged (but not mandatory)

SU-DRS02-2018-2019-2020 (1/2)

Technologies for first responders

Type of Action	Research & Innovation Action
Output TRL	4 to 6
Project duration	not specified
Budget per project	~7 M€
Total budget	21 M€ in 2018 ------ 21 M€ in 2019
Eligibility conditions	At least 3 first responders from 3 different EU or associated countries (or at least 5 first responders for the open sub-topic)
Deadline	23 Aug 2018 ------ 22 Aug 2019 ------ 27 Aug 2020

- Challenge
  - ❑ Resilience is critical to allow authorities to take proper measures in response to severe disasters.
  - ❑ Innovation for disaster-resilient societies may draw from novel technologies.

SU-DRS02-2018-2019-2020 - Scope (2/2)

Technologies for first responders

Protection of first responders, or enhancing their capacities by addressing related R&I issues, in particular:

1. Sub-topic 1: [2018] Victim-detection technologies
   - Novel technologies for quick detection of victims trapped in buildings to enable faster rescue operations
2. Sub-topic 2: [2019] Innovation for rapid and accurate pathogens detection
   - Novel technologies for the rapid detection of pathogens
   - Tools for joint epidemiological and criminal risk and threat assessment and investigation.
3. Sub-topic 3: [2020] Methods and guidelines for pre-hospital life support and triage
4. Sub-topic 4: [2018-2019-2020] Open - Technologies for use by first responders, including:
   - communicating and smart wearables * for first responders and canine units including light-weight energy sources;
   - situational awareness and risk mitigation systems for first responders using UAV and robots, connected and swarms of drones *; systems based on the internet of things *;
   - solutions based on augmented or virtual reality;
   - systems communication solutions between first responders and victims *;
   - risk anticipation and early warning technologies;
   - mitigation, physical response or counteracting technologies; etc.

- Tests and validation in training installations and through in-situ experimental deployment
- Contribution of first responders, including through interdisciplinary teams
  - involving medical emergency services, public health authorities, law enforcement team, civil protection professionals, etc.
- New methods to organise the interaction between first responders with researchers
- International cooperation, in particular with Korean or Japanese research centres, is encouraged

SU-DRS03-2018-2019-2020 (1/2)

Pre-normative research and demonstration for disaster resilient societies

Type of Action	Innovation Action
Output TRL	6 to 7
Project duration	not specified
Budget per project	6M€
Total budget	6 M€ in 2018 ------ 6 M€ in 2019 ------ 6 M€ in 2020
Eligibility conditions	At least 3 first responders from 3 different EU or associated countries
Deadline	23 Aug 2018 ------ 22 Aug 2019 ------ 27 Aug 2020

- **Challenge**
  - A reason for the difficult interaction among practitioners, lies in the insufficient harmonisation and standardisation, which pre-normative research and demonstrations may address effectively.

SU-DRS03-2018-2019-2020 - Scope (2/2)

Pre-normative research and demonstration for disaster resilient societies

Address issues related to pre-standarisation, in particular:

1. Sub-topic 1: [2018] Pre-standardisation for the security of water supply
   - Based on the legacy of FP7-funded actions,
     - Design clearer strategies to integrate current technologies in the existing water safety network
     - Interconnect the testing facilities of safety (e.g. contamination risks) and security (e.g. deliberate poisoning) related networks of sensors that are deployed
     - Demonstrate the use of current sensor technologies for the purpose of both safety and security of water, *including methods to monitor reservoirs, and sea or river levels for early warning*.

2. Sub-topic 2: [2019] Pre-standardisation in CBRN-E crisis management
   - Bring innovative, validated and positively-assessed practices into standards within or outside current standardisation processes.
   - Increase interoperability of CBRN equipment and procedures
   - Involve well-established standardisation organisations
   - Describe the complementarity of the proposed activities with activities supported by EDA

3. Sub-topic 3: [2020] First aids vehicles deployment, training, maintenance, logistic and remote centralized coordination means
   - standards for an effective deployment of resources to respond to major crisis.

SU-DRS04-2019-2020 (1/2)

Chemical, biological, radiological and nuclear (CBRN) cluster

Type of Action	Research & Innovation Action
Output TRL	4 to 8
Project duration	not specified
Budget per project	~3,5 M€
Total budget	10,5 M€ in 2019 (for 3 projects) ------ not yet defined for 2020
Eligibility conditions	- Each RIA proposal must be coordinated by an SME. - All beneficiaries must be independent from each beneficiary in ENCIRCLE. - Must establish a "Collaboration Agreement" with participant(s) in the ENCIRCLE. - A draft of the "Collaboration Agreement" must be attached to the RIA proposal, and endorsed by at least one participant in ENCIRCLE.
Deadline	23 Aug 2018 ------ 22 Aug 2019 ------ 27 Aug 2020

- **Challenge**

SME's often face difficulties in bringing CBRN products to markets because:

- they address local, small niche markets;
- They have neither the capabilities nor the strategic objective to go for foreign markets;
- The individual technologies can make it to the market only and need to be integrated and combined with other tools by other companies that have the capabilities and the strategy to market products abroad.

SU-DRS04-2019-2020 - Scope (2/2)

Chemical, biological, radiological and nuclear (CBRN) cluster

- The Commission will select several RIAs aiming at R&D of novel CBRN technologies identified in the catalogue that is updated by the ENCIRCLE project on a regular basis.
- Each of these actions will be led by an SME.
- Each consortium must establish an agreement with the participants in ENCIRCLE which must settle how the project result will be exploited and integrated into platforms managed by ENCIRCLE.
- Where applicable, describe the complementarity of the proposed activities with EDA projects

SU-DRS05-2019 (1/2)

Methodical demonstration of novel concepts for the management of pandemic crises

- **Type of Action** Innovation Action
- **Output TRL** not specified
- **Project duration** maximum **24 months**
- **Budget per project** 10 M€
- **Total budget** 10 M€ in 2019 (for one project)
- **Eligibility conditions** Organizations in charge of national planning in relations with pandemics preparedness, from at least 5 different EU or Associated countries.

  At least 3 first responders from 3 different EU or associated countries
- **Deadline** 22 Aug 2019
- **Challenge**
  - ❑ Large-scale pandemics constitute an ever growing threat in the globalized society and the increasing flows of goods and people among continents, which ought to be addressed internationally, and with the involvement of a large variety of practitioners, from planners in national health systems, to first responders.

SU-DRS05-2019 - Scope (2/2)

Methodical demonstration of novel concepts for the management of pandemic crises

- DRS-4-2014 addressed the feasibility of strengthening capacity-building for health and security protection in case of large-scale pandemics (phase 1). The resulting project
  - has issued a range of recommendations for research gaps to be addressed in priority
  - proposed innovative concepts to integrate the existing tools and systems for health and security protection in case of large-scale pandemics

  (these recommendations will be made public on the portal of the Call in due time)

- Provide a model emergency framework for health and security protection in the case of large-scale pandemics, validated by international organizations and a large number of EU Member States

- Provide a prototype IT system integrating innovative tools, and supporting the functions of the model emergency framework

- Demonstrate in situ these novel concepts for health and security protection in the case of large-scale pandemics, in support of cross-border emergency approaches (phase 2)

SU-FCT

Fight Against Crime and Terrorism

Fight against Crime

Fight against Terrorism

Call – SU-FCT

Mission:

The ambition of the activities under FCT is to mitigate potential consequences of crime and terrorism-related incidents or to avoid them.

New technologies and capabilities are required to fight against illegal trafficking and terrorism, along with understanding and tackling terrorist ideas and beliefs.

4 topics

1. SU-FCT01-2018-2019-2020:
   Human factors, and social, societal, and organisational aspects to solve issues in FCT

2. SU-FCT02-2018-2019-2020:
   Technologies to enhance the FCT

3. SU-FCT03-2018-2019-2020:
   Information and data stream management to fight against (cyber)crime and terrorism

4. SU-FCT04-2020:
   Explosives: detection, intelligence, forensics

SU-FCT : 2018 → 2020

Year	Topic (Type of Action)	Title	Budget (M€)	Deadline
2018	SU-FCT01-2018-2019-2020 (RIA) SU-FCT02-2018-2019-2020 (RIA) SU-FCT03-2018-2019-2020 (IA)	Human factors for FCT Technologies to FCT Information and data stream Mgt	10,0 21,0 8,0	23 Aug 2018
2019	SU-FCT01-2018-2019-2020 (RIA) SU-FCT02-2018-2019-2020 (RIA) SU-FCT03-2018-2019-2020 (IA)	Human factors for DRS Technologies to FCT Information and data stream Mgt	5,0 21,0 6,0	22 Aug 2019
2020	SU-FCT01-2018-2019-2020 (RIA) SU-FCT02-2018-2019-2020 (RIA) SU-FCT03-2018-2019-2020 (IA) SU-FCT04-2020 (RIA)	Human factors for DRS Technologies to FCT Information and data stream Mgt Explosives	5,0 21,0 8,0 10,0	27 Aug 2020

SU-FCT01-2018-2019-2020 (1/2)

Human factors, and social, societal, and organizational aspects to solve issues in fighting against crime and terrorism

Type of Action	Research & Innovation Action
Output TRL	not specified
Project duration	not specified
Budget per project	5 M€
Total budget	10 M€ in 2018 ------ 5 M€ in 2019 ------ 5 M€ in 2020
Eligibility conditions	At least 3 practitioners from 3 different EU or associated countries (or at least 5 practitioners for the open sub-topic)
Deadline	23 Aug 2018 ------ 22 Aug 2019 ------ 27 Aug 2020

- **Challenge**
  - ❑ Security is a key factor to ensure a high quality of life and to protect our infrastructure through preventing and tackling common threats.
  - ❑ The EU must play its part to help prevent, investigate and/or mitigate the impact of criminal acts, whilst protecting fundamental rights.

SU-FCT01-2018-2019-2020 - Scope (2/2)

Human factors … to FCT

The societal dimension of fight against crime and terrorism should be at the core of the proposed activities.

1. Sub-topic 1: [2018] Trafficking of human beings and child sexual exploitation (both phenomena should be addresses in parallel)

   - Ensure advances in SSH to assist victims and protect them against child sexual exploitation, and the trafficking of human beings which are facilitated by globalisation and technological developments.

   - Interdisciplinary approaches to both issues are recommended

   - Trafficking of human beings:
     - how to prevent the phenomenon, and to reduce the demand for all forms of exploitation in the trafficking chain
     - Analyse possible involvement of organized crime groups in other crimes (e.g., financial crimes)

   - Child sexual exploitation:
     - how to address new threats, such as live-streaming of child abuse and coercion and extortion of victims
     - how to provide law enforcement with effective means to detect, investigate and bring down the networks
     - how to help victims
     - how to reduce risks of (re-)offending by better understanding the behaviour of abusers and potential abusers

2. Sub-topic 2: [2019] Understanding the drivers of cybercriminality, and new methods to investigate and mitigate cybercriminality

   - The dissemination of "cybercrime-as-a-service" business models is an important enabler for crime and poses significant challenges to security → need to understand their trends

   - Human factors determining online behaviour, as often individuals feel disconnected from the actual crime or do not perceive it as a crime in the first place

   - Recent trends indicate also a growth in cyber juvenile delinquency and a rise in adolescent hacking. Research in domains such as psychology, criminology, anthropology, neurobiology and cyber psychology to better understand the factors contributing to it.

3. Sub-topic 3: [2020] Developing comprehensive multi-disciplinary and multi-agency approaches to prevent and counter violent radicalisation in the EU

4. Sub-topic: [2018] **Open**

SU-FCT02-2018-2019-2020 (1/2)

Technologies to enhance the fight against crime and terrorism

Type of Action	Research & Innovation Action
Output TRL	4 to 6
Project duration	not specified
Budget per project	~7 M€
Total budget	21 M€ in 2018 ------ 21 M€ in 2019 ------ 21 M€ in 2020
Eligibility conditions	At least 3 LEAs from 3 different EU or associated countries (or at least 5 LEAs for the open sub-topic)
Deadline	23 Aug 2018 ------ 22 Aug 2019 ------ 27 Aug 2020

- **Challenge**
  - Organized crime and terrorist organisations are often at the forefront of technological innovation in planning, executing and concealing their criminal activities and the revenues stemming from them.
  - LEAs are often lagging behind when tackling criminal activities supported by advanced technologies.

SU-FCT02-2018-2019-2020 - Scope (2/2)
Technologies … to FCT

Proposals should be submitted under only one of the following sub-topics:

1. Sub-topic 1: [2019] Trace qualification
   - Develop novel robotized or automated tools for forensic analysis: rapid and at an acceptable cost
   - Develop tools for a better interpretation of: trace composition, time when they were left, cause of their origin
2. Sub-topic 2: [2018] **Digital forensics in the context of criminal investigations** *
   - Develop new forensic tools, techniques and methodologies, based on common practices and standards, that allow for rapid retrieval, storage, analysis and validation of digital evidence (including on the cloud)
   - Enable investigations to identify perpetrators as well as victims (in particular in cases of child sexual abuses)
   - Focus on data gathering, data exploitation, and speedy exchange of information (all types of crime, terrorist activities and propaganda, and malicious acts by foreign-state perpetrators are concerned)
   - Research should take into account new and emerging trends (for instance, abuse of encryption for criminal or terrorist purposes), while fully respecting fundamental rights and privacy
3. Sub-topic 3: [2020] Money flows tracking
4. Sub-topic: [2018-2019-2020] **Open** *
   - E.g. technologies to improve LEAs capabilities; autonomous systems to improve the FCT; technologies to support better protection of public figures; tracking and monitoring technologies; capabilities to detect the widest possible range of threats and concealments (including complex concealed weapons)

SU-FCT03-2018-2019-2020 (1/2)

Information and data stream management to fight against (cyber)crime and terrorism

Type of Action	Innovation Action
Output TRL	5 to 7
Project duration	maximum **24 months**
Budget per project	8M€
Total budget	8 M€ in 2018 ------ 8 M€ in 2019 ------ 8 M€ in 2020
Eligibility conditions	At least 3 LEAs from 3 different EU or associated countries
Deadline	23 Aug 2018 ------ 22 Aug 2019 ------ 27 Aug 2020

- **Challenge**
  - ❑ A Large amounts of data and information from a variety of origins have become available to practitioners involved in fighting crime and terrorism.
  - ❑ Full advantage is not currently taken of the most advanced techniques for Big Data analysis, and artificial intelligence

SU-FCT03-2018-2019-2020 - Scope (2/2)

Information and data stream management to FCT *

- The internet of things connects practically everything, thus making everything more vulnerable as well. Wearable devices make us traceable, 3D printers can produce weapons, autonomous cars provide opportunities for kidnappers, teleworking opens doors for cyber-espionage etc.
- Cybercriminals follow the technological development and benefit from it, while measures for countering cybercrime are often one step behind.
- LEAs would benefit from new means of preventing and countering new kinds of crime
- Predictive analytics would greatly benefit from open source intelligence gathering, social network and darknet data analysis, and allow for resource-efficient, effective and proactive law enforcement.
- Behavioural/anomaly detection systems (using a large variety of sensors) and methodologies require the analysis and processing of enormous quantities of data, together with improved imaging techniques to allow for the identification of suspicous events or of criminals. Such systems should operate in near real-time and at similar distances as a surveillance camera.
- Convert voluminous and heterogeneous data sets (images, videos, geospatial intelligence, communication data, traffic data, financial transactions related date, etc.) into actionable intelligence
- Build consortia involving relevant security practitioners, civil society organisations, and the appropriate balance of IT specialists, psychologists, sociologists, linguists, etc. to exploit big data in order to
  a) caracterize trends in cybercrime and in cybercriminal organizations (based on a profound analysis of current and emerging cybercriminal organizational types and structures)
  b) enhance citizens' security against terrorist attacks in places considered as soft targets, including crowded areas (stations, shopping malls, entertainment venues, etc.).

SU-FCT04-2020

Explosives: detection, intelligence, forensics

Type of Action	Research & Innovation Action
Output TRL	not specified
Project duration	maximum **24 months**
Budget per project	10 M€
Total budget	10 M€ in 2019 (for one project)
Eligibility conditions	at least **6** relevant practitioners from at least 3 different EU or Associated countries
Deadline	22 Aug 2019

- **Challenge**
  - ❑ Terrorists and other criminals are constantly seeking new ways to develop, deploy, activate and detonate explosives. Their manufacturing methods evolve continuously, which makes the specialized work of law enforcement agencies (LEAs) in this area a continuous challenge.
  - ❑ R&D support needs to anticipate and match the next possible innovation to
    - ○ increase deterrence messaging
    - ○ increase the speed of the screening process
    - ○ reduce the cost to airports/airlines.

SU-BES

Border and External Security

Call – SU-BES

Mission:

The aim is to develop technologies and capabilities which are required to enhance systems and their interoperability, equipment, tools, processes, and methods for rapid identification to improve border security.

Technologies, capabilities and solutions are also required to support the Union's external security policies in civilian tasks.

3 topics

1. SU-BES01-2018-2019-2020:
   Human factors, and social, societal, and organisational aspects of BES

2. SU-BES02-2018-2019-2020:
   Technologies to enhance BES

3. SU-BES03-EBCGA-2018-2019-2020:
   Demonstration of applied solutions to enhance border and external security

SU-BES : 2018 → 2020

Year	Topic (Type of Action)	Title	Budget (M€)	Deadline
2018	SU-BES01-2018-2019-2020 (RIA) SU-BES02-2018-2019-2020 (RIA) SU-BES03-EBCGA-2018-2019-2020 (IA)	Human factors for BES Technologies for BES BES demo of applied solutions	10,0 21,0 10,0	23 Aug 2018
2019	SU-BES01-2018-2019-2020 (RIA) SU-BES02-2018-2019-2020 (RIA) SU-BES03-EBCGA-2018-2019-2020 (IA)	Human factors for BES Technologies for BES BES demo of applied solutions	5,0 21,0 10,0	22 Aug 2019
2020	SU-BES01-2018-2019-2020 (RIA) SU-BES02-2018-2019-2020 (RIA) SU-BES03-EBCGA-2018-2019-2020 (IA)	Human factors for BES Technologies for BES BES demo of applied solutions	tbd	27 Aug 2020

SU-BES01-2018-2019-2020 (1/2)

Human factors, and social, societal, and organizational aspects of border and external security

Type of Action	Research & Innovation Action
Output TRL	not specified
Project duration	not specified
Budget per project	5 M€
Total budget	10 M€ in 2018 ------ 5 M€ in 2019
Eligibility conditions	At least 3 border/coast guards from 3 different EU or associated countries (or at least 5 for the open sub-topic)
Deadline	23 Aug 2018 ------ 22 Aug 2019 ------ 27 Aug 2020

- **Challenge**
  - ❑ BES may depend on a variety of human factors, and social and societal issues. Deeper understanding of how novel technologies and social media impact border control are required.
  - ❑ One main challenge is to manage the flow of travellers and goods arriving at our external borders, while at the same time tackling irregular migration and enhancing our internal security.
  - ❑ Any novel technology or organisational measure will need to be accepted by the European citizens.

SU-BES01-2018-2019-2020 - Scope (2/2)

Human factors … of BES

1. Sub-topic 1: [2018] Detecting security threats possibly resulting from certain perceptions abroad, that deviate from the reality of the EU
   - Investigate how to better detect and understand how the EU is perceived in countries abroad by analysing e.g. social media data,
     - how such perception could lead to threats and security issues
     - how such perceptions can be avoided or counteracted
   - International cooperation is encouraged.
2. Sub-topic 2: [2019] Modelling, predicting, and dealing with migration flows to avoid tensions and violence
   - Better modelling and predicting migration flows, for high level strategic decision-making,
   - Map public sentiment, including perceptions of migration, by analysing data available from many different governmental or public sources, and by developing socio-economic indicators for the management of the migratory flow.
3. Sub-topic 3: [2020] Developing indicators of threats at the EU external borders on the basis of sound risk and vulnerabilty assessment methodologies
4. Sub-topic: [2018] Open

SU-BES02-2018-2019-2020 (1/3)

Technologies to enhance border and external security

- **Type of Action** Research & Innovation Action
- **Output TRL** 4 to 6
- **Project duration** not specified
- **Budget per project** ~7 M€
- **Total budget** 21 M€ in 2018 (3 projects per year) ------ 21 M€ in 2019

- **Eligibility conditions** At least 3 border/coast guards from 3 different EU or associated countries (or at least 5 for the open sub-topic)
- **Deadline** 23 Aug 2018 ------ 22 Aug 2019 ------ 27 Aug 2020

- **Challenge**
  - ❑ Innovation for border and external security may draw from novel technologies, provided that they are affordable.

SU-BES02-2018-2019-2020 - Scope (2/3)

Technologies to enhance BES

Proposals are invited to address related research and innovation issues, in particular:

- Sub-topic 1: [2018] Providing integrated situational awareness and applying augmented reality to border security
  - (Cloud-based) integrated systems
    - with highly-standardized interfaces
    - showing real-time information in a user-friendly way
    - can assist border guards in decision-making, and in remaining in contact with their command and control centre
  - Water, land and air operating resources should be taken into account
- Sub-topic 2: [2018] Detecting fraud, verifying document validity, and alternative technologies to identifying people *
  - Countermeasures are needed to address potential frauds, in particular for the detection of morphed face images.
  - Tools for the use of biometrics "on the fly" techniques for identification in a non-intrusive manner and without interrupting the flow of people
- Sub-topic: [2018-2019-2020] Open

SU-BES02-2018-2019-2020 - Scope (3/3)

Technologies to enhance BES

- Sub-topic 3: [2019] Security on-board passenger ships
    - New technologies to ensure security all along the "life cycle" of a voyage
    - Methods for the deployment and integration into ship systems
    - Novel procedures (including for embarkation and disembarkation, mooring at pier)

- Sub-topic 4: [2019] Detecting threats in the stream of commerce without disrupting business
    - Facilitate the detection of dangerous and illegal goods without disrupting business
        - by novel technologies and sensing strategies characterized by risk-based protection and non-intrusive security checks
    - Automation and integration of existing technologies to identify threat materials and to ensure the supervision of the logistic flow of goods.
    - Exploit information obtained through the analysis of cargo flow data available from open source and documentary control, intelligence gathering, risk management, as well as through physical detection or inspection of cargo in means of transport, luggage, or carried by individuals.
    - Of particular relevance:
        - the enhancement of detection capabilities of contraband (mainly cigarettes) hidden in high density cargo in particular for rail cargo transport,
        - the figtht against illicit trafficking of radioactive and nuclear (NR) materials

- Sub-topic 5: [2020] Disruptive sensor technologies for border surveillance

SU-BES03-EBCGA-2018-2019-2020 (1/2)

Demonstration of applied solutions to enhance border and external security

Type of Action	Innovation Action
Output TRL	6 to 8
Project duration	maximum **18 months**
Budget per project	5M€
Total budget	10 M€ in 2018 ------ 10 M€ in 2019
Exceptional funding rates	Cost of fuel is excluded from the costs eligible
Eligibility conditions	At least 3 border/coast guards from 3 different EU or associated countries (or at least 5 for the open sub-topic) Consortia must be coordinated by a practitioner under civilian authority
Deadline	23 Aug 2018 ------ 22 Aug 2019 ------ 27 Aug 2020

- **Challenge**
  - ❑ BES solutions at high TRL exist but they need to be demonstrated in the context of actual operations

A delegation agreement covering the 2018-2020 activities will be concluded between the Commission and the European Border and Coast Guard Agency (EBCGA)

SU-BES03-EBCGA-2018-2019-2020 - Scope (2/2)

Demonstration of applied solutions to enhance BES

1. Sub-topic 1: [2018] Remotely piloted aircrafts and underwater autonomous platforms to be used from on-board offshore patrol vessels
   - Remotely piloted autonomous platforms for land border and coast surveillance.
   - Underwater autonomous platforms for choke points surveillance (i.e. a port entrance.)
   - Research on artificial intelligence to facilitate the transition from innovation to operation
   - Contribute to better situational awareness at the tactical level beyond coastal waters (up to 200 nautical miles)
     - by increasing the performance of existing technologies
     - or by developing innovative concepts of operation
   - Improve the on-board processing of payload data to minimize the data transmission to the ground segment

2. Sub-topic 2: [2019] New concepts for decision support and information systems
   - Information systems to support border and external security
   - Exploit data for their use in surveillance
   - Ensure the interoperability of surveillance systems, and the availability of information for maritime border surveillance
   - Allow faster reaction to incidents in themaritime domain, and a reduction in the death toll at sea.

3. Sub-topic 3: [2020] Improved systems for the detection, identification and tracking of small boats

4. Sub-topic: [2018-2019-2020] Open

Demonstrate the complementary with the PADR-US-01-2017 topic:

Technological demonstrator for enhanced situational awareness in a naval environment.

SU-GM

General Matters

Call – SU-GM

3 topics

1. SU-GM01-2018-2019-2020:
   Pan-European networks of practitioners and other actors in the field of security

2. SU-GM02-2018-2020:
   Strategic pre-commercial procurements of innovative, advanced systems to support security

3. SU-GM03-2018-2019-2020:
   Pre-commercial procurements of innovative solutions to enhance security

SU-GM : 2018 → 2020

Year	Topic (Type of Action)	Title	Budget (M€)	Deadline
2018	SU-GM01-2018-2019-2020 (CSA) SU-GM02-2018-2020 (CSA) SU-GM03-2018-2019-2020 (PCP)	Networks of practitioners PCP of innovative & advanced systems PCP of innovative solutions	5,0 6,0 7,0	23 Aug 2018
2019	SU-GM01-2018-2019-2020 (CSA) SU-GM03-2018-2019-2020 (PCP)	Networks of practitioners PCP of innovative solutions	10,5 7,0	22 Aug 2019
2020	SU-GM01-2018-2019-2020 (CSA) SU-GM02-2018-2020 (PCP) SU-GM03-2018-2019-2020 (PCP)	Networks of practitioners PCP of innovative & advanced systems PCP of innovative solutions	tbd	27 Aug 2020

SU-GM01-2018-2019-2020 (1/3)

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

Type of Action	Coordination & Support Action
Project duration	**5 years**
Budget per project	3,5 M€ except for sub topic c) 1,5M€
Total budget	5 M€ in 2018 ------ 10,5 M€ in 2019 ------ 7 M€ in 2020
Eligibility conditions	- At least 8 practitioners from 8 different EU or associated countries - Must include a dissemination work package, including an annual workshop/conference - Part a) 25% of the total cost of the action, to interact with industry and academia - Only one network by category may be supported over the 2018-2019 period – more details about the eligible professional areas will be provided
Deadline	23 Aug 2018 ------ 22 Aug 2019 ------ 27 Aug 2020

- **Challenge**
  - ❑ Practitioners interested in the uptake of security research and innovation are dedicated to performing their duty and are focused on their tasks.
  - ❑ Practitioner organisations have little scope to free workforces from daily operations in order to allocate time and resources to monitor innovation and research that could be useful to them.
  - ❑ They have few opportunities to interact with academia or with industry on such issues.

SU-GM01-2018-2019-2020 - Scope (2/3)
Pan-European networks of practitioners

Practitioners are invited to associate in 4 different categories of networks in the field security:

b) [2018] Innovation clusters from around Europe (established at national, regional or local level), managing demonstration sites, testing workbenches, and training facilities (including those providing simulators, serious gaming platforms, testing of Public Protection and Disaster Relief (PPDR) applications on broadband networks) in order to

1) establish and maintain a roster of capabilities and facilities
2) organise to share expertise
3) plan to pool and share resources with a view to facilitating access to their respective facilities among collective membership when this would constitute an economy of scale and allow a more intensive use of expensive equipment
4) coordinate future developments and workbenches' acquisition

c) [2018] Procurement agencies, or departments, active at budgeting and implementing the acquisition of security solutions at European, national, regional or local level can get together to:

1) share investment plans,
2) compare procurement techniques and rules
3) plan for common procurements of research services as well as of innovative, off-the-shelf products

SU-GM01-2018-2019-2020 - Scope (3/3)
Pan-European networks of practitioners

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,
2. to express common requirements
3. to indicate priorities as regards areas requiring more standardization

In 2019, proposals are invited in two specific areas of specialisation: the protection of public figures; the handling of hybrid threats.

d) [2019] Border and coast guard organisations, procurement authorities, industry and researchers are invited to draft the roadmaps to provide innovative, future solutions for border and coast surveillance, control and management, in the context of integrated border management and "dematerialised" borders.

A roadmap for border and coast guard authorities, and industry, to plan ahead and to facilitate future investments into common, interoperable solutions and systems.

SU-GM02-2018-2020 *(CSA & PCP)* (1/2)

Strategic pre-commercial procurements of innovative, advanced systems to support security

Type of Action	for sub-topic 1 year 2018) Coordination & Support Action in 2018
	for sub-topic 2 year 2020) Cofund Pre Commercial Procurement in 2020

Output TRL	not specified but should be 7 to 8 for sub-topic 2
Project duration	not specified
Budget per project	1 M€
Total budget	6 M€ in 2018 (6 projetcs)
Funding rates	for sub-topic 2, **90%** of the total eligible costs
Eligibility conditions	Sub-topic 1): at least 6 practitioners and 3 "buyers", from 3 different EU or AC Sub-topic 2): at least 3 practitioners and 3 "buyers", from 3 different EU or AC
Deadline	23 Aug 2018 ------ 22 Aug 2019 ------ 27 Aug 2020

- **Challenge**
  - ❑ Innovative solutions must support the EU when national resources are required to work more closely together.

SU-GM02-2018-2020 *(CSA & PCP)* - Scope (2/2)
Strategic PCP of innovative, advanced

- Sub-topic 1: [2018] Common requirements specifications for innovative, advanced systems to support security
  - Work on common requirements of any kind of system that practitioners may need to
    - enhance border and external security
    - fight against crime and terrorism
    - protect infrastructure
    - make societies more resilient
    - involve their respective procurement bodies in preparing for future acquisitions
  - Proposals must necessarily state:
    1) Agreement from participating procurement authorities to negotiate, in good faith and on a case-by-case basis, with non-participating procurement authorities that wish to procure a capability or a product derived from this action
    2) Commitment from participating procurement authorities to consult with any legal entity generating information to be released
    3) Commitment from participating procurement authorities to negotiate the use granted on Fair Reasonable and Non-Discriminatory (FRAND) terms

- Sub-topic 2: [2020] Procurement of prototype systems among those specified as a result of Sub-topic 1

SU-GM03-2018-2019-2020 (1/2)

Pre-commercial procurements of innovative solutions to enhance security

Type of Action	Cofund Pre Commercial Procurement
Output TRL	8
Project duration	not specified
Project size	2 to 12 M€ *(see the funding rate)*
Total budget	7 M€ in 2018 ------ 7 M€ in 2019
Funding rates	limited to **70%** of the eligible costs. Applicants may request a lower funding rate, so as to increase the leveraging effect
Eligibility conditions	At least 3 practitioners and 3 "buyers", from 3 different EU or AC
Deadline	23 Aug 2018 ------ 22 Aug 2019 ------ 27 Aug 2020

- **Challenge**
  - Innovative solutions must support the European Union when its national resources are required to work more closely together when engaged in actions to improve security

SU-GM03-2018-2019-2020 - Scope (2/2)
PCP of innovative solutions

- Proceed with the procurement of innovative solutions to enhance the practitioner operational capability
  - Phase 0: To draft common requirements for innovative prototypes, and to prepare the technical tender documents
  - Phase 1: To prepare a full tenders package for calls for tenders to build security-relevant prototypes
  - Phase 2: To implement the calls for tenders to generate 2 prototypes from 2 different sources
  - Phase 3: To benchmark and validate the 2 prototypes against the method developed during Phase 1
  - Phase 4: To draft a curriculum for pan European training in using the prototypes

SU-DS

Digital Security
Cybersecurity and Digital Privacy

Call – SU-DS

151 M€ for 2018-19-20

Mission:

The aim is to make the society as a whole benefitting from
user-friendly systems on cybersecurity, digital privacy and personal data protection,
enabling an active participation of citizens and organisations to their own security, privacy and personal data protection.

5 topics

1. SU-DS01-2018:
   Cybersecurity preparedness - cyber range, simulation and economics
2. SU-DS02-2020:
   Management of cyber-attacks and other risk
3. SU-DS03-2019-2020:
   Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises
4. SU-DS04-2018-2020:
   Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks
5. SU-DS05-2018-2019:
   Digital security, privacy and accountability in critical sectors

SU-DS : 2018 → 2020

Year	Topic (Type of Action)	Title	Budget (M€)	Deadline
2018	SU-DS01-2018 (IA) SU-DS04-2018-2020 (IA) SU-DS05-2018-2019 (IA)	Cybersecurity preparedness Electrical Power and Energy System Critical sectors: Privacy Accountability	16,0 20,0 8,5	23 Aug 2018
2019	SU_DS03-2019-2020 (IA) SU-DS05-2018-2019 (**RIA**) SU-DS05-2018-2019 (**IA**)	Digital Security and privacy Critical sectors: Privacy Accountability Critical sectors: Privacy Accountability	18,0 10,0 10,0	22 Aug 2019
2020	SU-DS02-2020 (IA) SU-DS03-2019-2020 (IA) SU-DS04-2018-2020 (IA)	Management of cyber-attacks Digital Security and privacy Electrical Power and Energy System	38,0 10,8 20,0	27 Aug 2020

SU-DS01-2018 (1/3)

Cybersecurity preparedness - cyber range, simulation and economics

Type of Action	Innovation Action
Output TRL	7
Budget per project	5 to 6 M€
Total budget	16 M€ in 2018 (3 projects)
Deadline	23 Aug 2018

- **Challenge**
  - ❑ digital infrastructure must be resilient and trustworthy, and must remain secure despite the escalating cyber-threats. New technologies require innovative ways to implement security measures
    - ❑ making new security-related assumptions, identifying "zero day" vulnerabilities or potential unknown vulnerabilities, forecasting new threats plus their cascading effects and emerging attacks, as well as managing cyber risks.
  - ❑ Many organisations are unable to forecast and/or estimate the impacts (e.g. economic, reputational, legal, social, business, societal) of a cyber-risk (e.g. data breach).
  - ❑ This results often in insufficient or wrong investments to ensure a more cyber secure environment.

SU-DS01-2018 - Scope (2/3)

Cybersecurity preparedness - cyber range, simulation and economics

- Extended capabilities of cyber ranges as a continuation of topic DS-07-2017
  - piloting of networked cyber-ranges;
  - extension of the cyber-ranges network,
  - adding domain specificities like cyber range for IoT and/or SCADA
- Develop, test and validate highly customizable dynamic simulators
  - knowledge-based platforms
  - mechanisms for real time interactions and information sharing
  - feedback loops
  - handling and forecasting security incidents, complex attacks and propagated vulnerabilities, based upon targeted scenarios and exercises
  - Bring shared approaches to express user needs into actual experiments and cyber exercises
  - Develop/integrate/parameterise appropriate tools and methods (e.g. modelling, gaming, dynamic decision making, extended dynamic vulnerability databases, attack ontologies/taxonomies) to build simulation scenarios.
  - Validate the proposed cyber-range model across one critical economic sector, involving as many as possible relevant stakeholders from its supply chain.

SU-DS01-2018 - Scope (3/3)

Cybersecurity preparedness - cyber range, simulation and economics

- Address the specific needs of end-users, private and public security end-users alike.
- Create operational links to the CERTs / CSIRTs network across the EU.
- Develop, test and validate operational ways to continuously analyse the information collected by CERT and/or CSIRT centres
- Feed the risk analysis models in order to derive appropriate econometric models that should help in:
  - a) identifying affordable security controls that are needed to protect valuable organization assets,
  - b) promoting the development of cyber insurance and liability policies/contracts
  - c) fostering service level agreements addressing security, privacy and personal data protection requirements and policies.
  - d) identifying the cost and time to recover following a cyber-attack
- Solutions for specific social aspects of digital security related to training, practical, operational, hands-on training, including:
  - i. increase the dynamics of the training and awareness methods,
  - ii. integrate awareness into the eco-system of humans, competences, services and solutions which are able to rapidly adapt to the evolutions of cyber attackers or even surpass them
- Participation of SMEs is strongly encouraged.

SU-DS02-2020

Management of cyber-attacks and other risk

Type of Action	Innovation Action

Not available yet in the work programme

Output TRL	
Project duration	
Budget per project	M€
Total budget	xx M€ in 2020
Deadline	23 Aug 2018

- **Challenge**
  - ❑ xxx

SU-DS03-2019-2020 (1/2)

Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises

Type of Action	Innovation Action
Output TRL	7
Budget per project	4 to 5 M€ for sub-topic 1 3 to 4 M€ for sub-topic 2
Total budget	18 M€ in 2019 ------ 10,8 M€ in 2020
Deadline	22 Aug 2019 ------ 27 Aug 2020

- **Challenge**
  - ❑ To protect personal data, people should be enabled to assess the cybersecurity risk and configure their own security, privacy and personal data protection
  - ❑ Most SMEs & MEs lack sufficient awareness and can only allocate limited resources -both technical and human- to counter cyber risks, hence they are an easier target.
  - ❑ Taking into account the significant economic role of SMEs & MEs in the EU, tailored research to innovation should support cybersecurity for SMEs & MEs

SU-DS03-2019-2020 - Scope (2/2)

Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises

Sub-topic 1: Protecting citizens' security, privacy and personal data protection

- Bring innovative solutions to personal data protection, help citizens to better monitor and audit their personal data protection
- Approaches, techniques and use-friendly tools for:
  1. improving resilience against privacy
  2. identifying, removing and reporting potential harmful content
  3. exercising citizens' right to erasure ("right-to-be-forgotten")
  4. informing citizens about their privacy and personal data protection level and empowering them to modulate it at any moment of their digital activities …

Sub-topic 2: Small and Medium-sized Enterprises and Micro Enterprises (SMEs&MEs): defenders of security, privacy and personal data protection

- Develop targeted, user-friendly and cost-effective solutions enabling SMEs&MEs to:
  - a) dynamically monitor, forecast and assess their security, privacy and personal data protection risks ;
  - b) become more aware of vulnerabilities, attacks and risks that influence their business
  - c) manage and forecast their security, privacy and personal data protection risks in an easy/affordable way
  - d) build on-line collaboration between SMEs & MEs associations and with CERTs/CSIRTs, enabling thus individual SMEs & MEs to report any incident.

SU-DS04-2018-2020 (1/2)

Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks *

Type of Action	Innovation Action
Output TRL	7
Budget per project	6 to 8 M€
Total budget	20 M€ in 2018 ------ 20 M€ in 2020 (Half of the budget is originated from Societal Challenge 3)
Deadline	23 Aug 2018 ------ 27 Aug 2020

- **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,
  - ❑ EPES will face an increasing range of threats requiring an attentive evaluation of the cyber security risk
  - ❑ Without appropriate cyber-defence measures, systems access could be violated and may cause power outages, damages and cascading effects to interconnected systems
  - ❑ To pursue the integration of the renewables within the existing EPES and to ensure that it benefits from the advantages brought by a modern digitalised electricity grid, there is a need for new security approaches.

SU-DS04-2018-2020 - Scope (2/2)

Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks

- Implement the following series of activities
  - i. defining cybersecurity design principles and standards with a set of common requirements to inherently secure EPES
  - ii. assessing vulnerabilities and threats of the system in a collaborative manner (involving all stakeholders in the energy provision supply chain)
  - iii. on that basis, designing a cyber-secure system architecture describing the advantages of the solution adopted compared to others and which guarantees the level of cybersecurity vital for EPES
  - iv. implementing both organisational and technical measures in real life demonstration testing the cyber resilience of the system with simulation of different types of attacks and severity
  - v. demonstrating the effectiveness of the measures with a cost-benefit analysis.
  - vi. develop security information and event management system collecting logs and other security-related documentation for analysis that can also be used for information sharing across operators of essential infrastructures and CERT
  - vii. formulate recommendations for standardisation and certification in cybersecurity at component, system and process level;
  - viii. propose policy recommendations on EU exchange of information.
- Pilot/demonstrator shall be at city level, involving generators, one primary substation, secondary substations and end users.
- Shall include the following types of entities: TSO, DSO, electricity generators, utilities, equipment manufacturers, aggregators, energy retailers, and technology providers.

SU-DS05-2018-2019 (1/2)

Digital security, privacy and accountability in critical sectors

Sub-topic 1 (2019): Digital security and privacy in multimodal transport

Type of Action	Innovation Action
Output TRL	7
Budget per project	5 M€
Total budget	xx M
Deadline	23 Aug 2018

Sub-topic 2 (2019): Digital security and privacy in healthcare ecosystem

Type of Action	Research & Innovation Action
Output TRL	7
Budget per project	5 M€
Total budget	xx M
Deadline	22 Aug 2019

Sub-topic 3 (2018): Digital security and privacy in finance

- 3-4 M€/projet
- IA: TRL 7

Type of Action	Innovation Action
Output TRL	7
Budget per project	3 to 4 M€
Total budget	xx M
Deadline	23 Aug 2018

- Challenge In critical vertical sectors, cybersecurity technologies should be aligned to the specific domain needs…

SU-DS05-2018-2019 - Scope (2/2)

Digital security, privacy and accountability in critical sectors

Sub-topic 1 [2019]: Digital security, privacy and personal data protection in multimodal transport

- Proposals under this sub-topic should focus on at least one of the following items:
  a. Secure access management for citizens to all types of vehicles. Novel tailored approaches related to cybersecurity by design in transportation systems
  b. Assurance and protection against specific cyber-attacks in the multimodal transport domain, addressing interconnected threats and propagated vulnerabilities
  c. Develop practical means for relevant on-line sharing information and distributing real-time security, privacy and data protection warnings to all stakeholders in the multimodal transport ecosystem (collaboration with CERTs/CSIRTs is highly encouraged).
  d. Standardization to allow the quick adoption of cybersecurity best practices in the domain
  e. Evaluate the feasibility of a security labelling for transportation.

SU-ICT

Cybersecurity

Call – SU-ICT

Mission:

Build trust among Member States and industry by fostering cooperation at **early stages in the research** and innovation process.

Pave the way for a competitive, trustworthy **Digital Single Market**.

4 topics

1. **SU-ICT-01-2018:**
   Dynamic countering of cyber-attacks

2. **SU-ICT-02-2020:**
   Building blocks for resilience in evolving ICT systems

3. **SU-ICT-03-2018:**
   Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap

4. **SU-ICT-04-2019:**
   Quantum Key Distribution testbed

SU-ICT : 2018 → 2020

Year	Topic (Type of Action)	Title	Budget (M€)	Deadline
2018	SU-ICT-01-2018 (IA)	Dynamic countering of cyber-attacks	40,0	28 Aug 2018
2019	SU-ICT-03-2018	Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap	50,0	29 May 2018
2020	SU-ICT-04-2019 (IA)	Quantum Key Distribution testbed	15,0	14 Nov 2018
	???	???		22 Aug ? 19 Nov? 2019

SU-ICT-01-2019 (1/3)

Dynamic countering of cyber-attacks

Type of Action	Innovation Action
Output TRL	6
Project duration	**not defined**
Budget per project	4 to 5 M€
Total budget	40 M€ (~10 projects)
Deadline	28 August 2018

- **Challenge**
  - ❑ Prevention and protection against attacks that target modern ICT components, complex ICT infrastructures and emerging technologies (e.g. IoT) remains a difficult task.
  - ❑ The increase of encrypted flows over the Internet should lead to adopt new techniques for detection of suspicious cyber activities and traffic patterns, and for classification of flows, while keeping privacy and confidentiality.
  - ❑ Another challenge is to use machine learning and analytics for cybersecurity.

SU-ICT-01-2019 - Scope (2/3)

*Dynamic countering of cyber-attacks – **strand a***

Strand a: Cyber-attacks management - advanced assurance and protection

- Holistic approaches for system configuration in order to minimize attack surfaces
- Trusted and verifiable computation systems and environments
- Secure runtime environments
- Assurance, advanced verification tools
- Secure-by-design methods
- Proposals
- should explore how artificial intelligence, deep learning can be used to fight against cyber-attacks and optionally for cyber threat intelligence to identify malicious activity
- may cover secure execution environments that ensure an adequate level of security, privacy and accountability
  - the execution platforms, the operating systems, the security supporting services, the authentication/access control mechanisms
- are encouraged to provide mechanisms for informing the users on their security/privacy levels, for providing warnings and assisting them in handling security and privacy related incidents.
- ✓ This may entail a whole series of activities, including behavioural, social and human aspects in the engineering process until developed systems and processes address the planned security/privacy/accountability properties.

Highly dynamic behaviours are the technical ***challenges*** generated by:

- Complexity of heterogeneous collections of hardware and software components.
- Complex ICT infrastructures. Emerging technologies (e.g. IoT).
- Diversity of development contexts and of levels of maturity
- Growing means of networked interactions
- Massive exchange of information and data
- Varied schedules of systems lifecycles
- Increased encrypted flows over the Internet

SU-ICT-01-2019 - Scope (3/3)

Dynamic countering of cyber-attacks – ***strand b***

Strand b: Cyber-attacks management - advanced response and recovery

- Capabilities to dynamically support human operators (e.g. Incident Response professionals)
- Capabilities should include:
  - Assessment how attacks propagate (e.g. attack-defence graphs and information visualization)
  - Measures to withstand and recover from a threat/attack,
  - Measures beyond cyber that can be needed (e.g. security policies)

Proposals should

- address the use of appropriate threat intelligence sources
- contribute to share information with relevant parties (e.g. Computer Security Incident Response Teams)
- explore forensics, penetration testing, investigation and attack attribution services
- provide mechanisms for informing the users on their security/privacy levels

Approaches can include

- combination of massive data and logs collection from various sources (e.g. network traffic, dark web, data coming from social networks such as pictures, tweets, discussions on forum) to facilitate investigation on security alerts and to find suspicious files trajectories in order to have the most appropriate response.
- efficient handling (e.g. classification, anomaly detection) of encrypted network traffic

SU-ICT-03-2018 (1/2)

Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap

- ❑ Scale up existing research for the benefit of the cybersecurity of the Digital Single Market, with solutions that can be marketable.
- ❑ Participants should propose, test, validate and exploit the possible organisational, functional, procedural, technological and operational setup of a cybersecurity competence network with a central competence hub.
- ❑ Set-up of the Cybersecurity Competence Network with a European Cybersecurity Research and Competence Centre
- ❑ Consortia of competence centres in cybersecurity to engage together in:
  - ❑ Common research, development and innovation in next generation industrial and civilian cybersecurity technologies (including dual-use), applications and services; focus should be on horizontal cybersecurity technologies as well as on cybersecurity in critical sectors (e.g. energy, transport, health, finance, eGovernment, telecom, space) ;
  - ❑ Strengthening cybersecurity capacities across the EU and closing the cyber skills gap;
  - ❑ Supporting certification authorities with testing and validation labs equipped with state of the art technologies (e.g. HPC, AI, Quantum, Blockchain) and expertise

SU-ICT-03-2018 - Scope (2/2)

Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap

- **Type of Action** Research and Innovation Action
- **Output TRL** **not defined**
- **Project duration** **not defined**

- **Budget per project** 16 M€
- **Total budget** 50 M€ (~3 projects)
- **Eligibility conditions** The consortium in a proposal must involve at least 20 partners
  should also engage industrial communities/stakeholders from various (not less than 3) sectors
  (e.g. telecom, finance, transport, eGovernment, health, space, defence) that will be involved in the demonstrations
- **Deadline** 29 Mai 2018
- **Challenge**
  - ❑ There is an urgent need to step up investment in technological advancements that could make the EU's digital Single Market more cybersecure and to overcome the fragmentation of EU research capacities.
  - ❑ Europe has to master the relevant cybersecurity technologies from secure components to trustworthy interconnected IoT ecosystems and to self-healing software.

SU-ICT-04-2019 (1/2)

Quantum Key Distribution testbed

Type of Action	Innovation Action
Output TRL	not defined
Project duration	not defines
Budget per project	15 M€
Total budget	15 M€ in 2018 (1 project)
Deadline	22 Aug or 19 Nov 2019 ???

- **Challenge**
  - Current security of the digital infrastructures and services will soon be under threat.
  - Confidentiality of data and communications, authentication, as well as the long-term integrity of stored data have to be guaranteed, even in the advent of quantum computers.
  - Introducing Quantum Key Distribution (QKD) in the underlying infrastructure has the potential to maintain end-to-end security in the long-term.

SU-ICT-04-2019 - Scope (1/2)
Quantum Key Distribution testbed

- Build an experimental platform based on trusted nodes to test and validate the concept of end-to-end security, providing quantum key distribution as a service.
- Develop an open, robust, reliable and fully monitored metropolitan area testbed network (ring or mesh configuration).
- Integrate equipment, components, protocols and network technologies with QKD systems and current digital security and communication networks.
- Demonstrate resistance against known hacking techniques, including quantum hacking techniques
- Make use of existing network infrastructure (fibres and/or satellites)
- Provide a quantum key exchange rate of at least 1Mbit/s at a distance of 40km and demonstrate how it responds to concrete application needs.
- Demonstrate different applications and use cases of QKD, optimizing end-to-end security rather than the security of individual elements.