Horizon 2020 - Secure Societies
2019 Calls

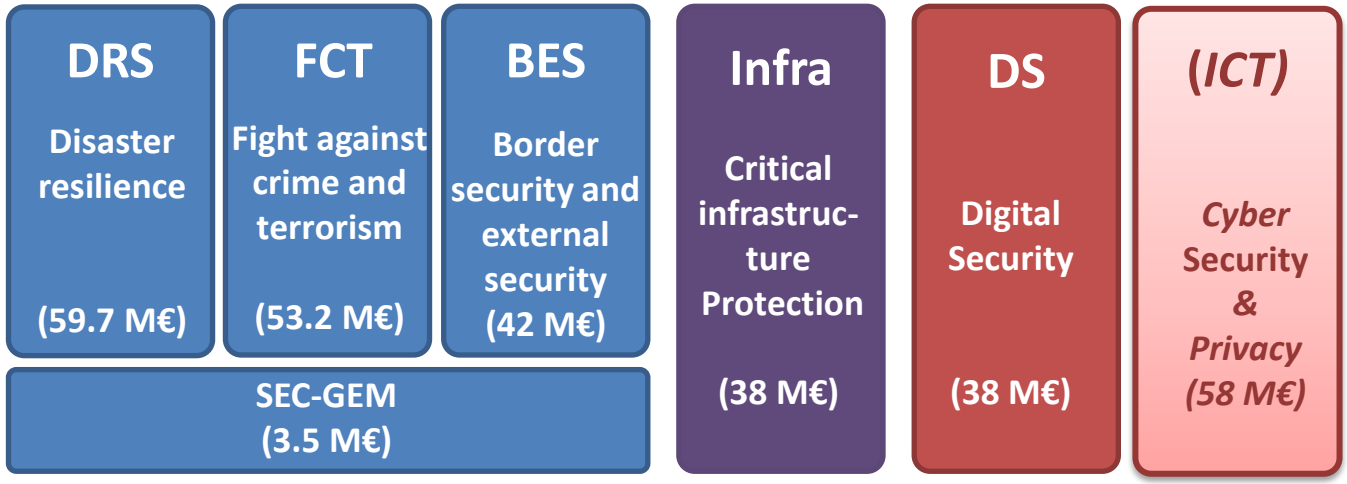
Infoday and brokerage event Riga, 9 April 2019

Armand Nachef (CEA)

The Horizon 2020 Security Union Topics of 2019

Co-funded by the Horizon 2020
Framework Programme of the European Union

Horizon 2020 Security
2019 Budget (292.4 M€)



Co-funded by the Horizon 2020
Framework Programme of the European Union

SC7 Call for proposals – 2019

SU-INFRA

Physical and cyber threats to critical infrastructure
SU-INFRA01 **(IA)**

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

SU-DRS

Human factors for DRS
SU- DRS01**(RIA)**

Technologies for first responders
SU- DRS02 **(RIA)**

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

CBRN cluster
SU- DRS04 **(RIA)**

Management of pandemic crises
SU- DRS05 **(IA)**

SU-FCT

Human factors to FCT
SU- FCT01 **(RIA)**

Technologies to FCT
SU- FCT02 **(RIA)**

Information and data stream Mgt
SU- FCT03 **(IA)**

SU-BES

Human factors for BES
SU- BES01 **(RIA)**

Technologies for BES
SU- BES02 **(RIA)**

Demo of applied solutions
SU- BES03 **(IA)**

SU-GM

Networks of practitioners
SU- GM01 **(CSA)**

SU-DS

Privacy for SMEs and citizens
SU- DS03 **(IA)**

accountability in critical sectors
SU- DS05 **(RIA) (IA)**

SU-ICT

Building blocks for resilience
SU- ICT-02-**2020** **(RIA)**

~~**Security and resilience for collaborative manufacturing environments**~~
ICT-08 **(RIA)**

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

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-INFRA

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

Protecting the Infrastructure

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-INFRA01-2018-2019-2020

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** 22 M€ in 2019
- **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** 22 Aug 2019
- **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.

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-INFRA01-2018-2019-2020 - Scope

Forecast, assess **physical and cyber risks**, prevent, detect, response, mitigate consequences, and achieve fast recovery

Share information with the public in the vicinity of the installations 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
   - 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 the risk assessment approach using specific examples and scenarios of real life

One of the following critical infrastructures that is not financed in 2018:

- Water systems
- Energy infrastructure (Energy value chain, Gas networks, **others**)
- Transport infrastructure (Ports, Airports, **others**)
- Communication infrastructure
- **Ground segments of space systems**
- Health services
- **E-Commerce and postal infrastructure**
- Sensitive industrial sites and plants
- Financial services

Objective:

- To cover the largest possible spectrum of installations.
- Minimize overlapping with ongoing actions
- **Areas in green are not yet covered**

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-INFRA02-2019

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
    - 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
  - Distinct smart technological and communication environments (urban, transport infrastructures, companies, industry) within a smart city require a common cybersecurity management approach.

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-INFRA02-2019 - Scope

- 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.

- Address at least one of the following key issues:
  A. Simulation and analysis of the security threats and risks of the interconnected 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

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-DRS

Disaster-Resilient Societies

Resilience

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-DRS01-2018-2019-2020

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 2019
- **Eligibility conditions** At least 3 first responders from 3 different EU or associated countries
- **Deadline** 22 Aug 2019

- **Challenge**
  - The resilience of societies heavily rely 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

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-DRS01-2018-2019-2020 - Scope

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)

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-DRS02-2018-2019-2020

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 2019
- **Eligibility conditions** At least 3 first responders from 3 different EU or AC (or at least 5 first responders for the open sub-topic)
- **Deadline** 22 Aug 2019

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

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-DRS02-2018-2019-2020 - Scope

Technologies for first responders

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

- 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.

- 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.

- International cooperation, in particular with Korean or Japanese research centres, is encouraged

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-DRS03-2018-2019-2020

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 2019

- **Eligibility conditions** At least 3 first responders from 3 different EU or associated countries
- **Deadline** 22 Aug 2019
- **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.

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-DRS03-2018-2019-2020 - Scope

Pre-normative research and demonstration for disaster resilient societies

Address issues related to pre-standarisation, in particular:

- Sub-topic 2: [2019] Pre-standardisation in crisis management (including natural hazard and CBRN-E emergencies)
  - 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

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-DRS04-2019-2020

Chemical, biological, radiological and nuclear (CBRN) cluster

- **Type of Action** Research & Innovation Action
- **Output TRL** 4 to 6
- **Project duration** not specified
- **Budget per project** ~3,5 M€
- **Total budget** 10,5 M€ in 2019 (for 3 projects)

- **Eligibility conditions**
  - Each RIA proposal must be coordinated by an SME.
  - All beneficiaries must be independent ENCIRCLE beneficiaries
  - Must establish a "Collaboration Agreement" with ENCIRCLE
- **Deadline** 22 Aug 2019
- **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

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-DRS04-2019-2020 - Scope

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

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-DRS05-2019

Methodical demo. 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 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.

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-DRS05-2019 - Scope

Methodical demo. 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).
- 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)

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-FCT

Fight Against Crime and Terrorism

Fight against Crime

Fight against Terrorism

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-FCT01-2018-2019-2020

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 2019
- **Eligibility conditions** At least 3 practitioners from 3 different EU or associated countries (or at least 5 practitioners for the open sub-topic)
- **Deadline** 22 Aug 2019

- **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.

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-FCT01-2018-2019-2020 - Scope

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 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.

2. Sub-topic: [2019] **Open**

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-FCT02-2018-2019-2020

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** 28,16 M€ in 2019

- **Eligibility conditions** At least 3 LEAs from 3 different EU or associated countries (or at least 5 LEAs for the open sub-topic)
- **Deadline** 22 Aug 2019

- **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.

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-FCT02-2018-2019-2020 - Scope

Technologies to enhance the fight against crime and terrorism

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

- Sub-topic 1: [2019] Trace qualification
  - Develop novel robotized/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

- 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)

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-FCT03-2018-2019-2020

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 2019

- **Eligibility conditions** At least 3 LEAs from 3 different EU or associated countries
- **Deadline** 22 Aug 2019

- **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

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-FCT03-2018-2019-2020 - Scope

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, 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 intelligence

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-BES

Border and External Security

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-BES01-2018-2019-2020

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 2019
- **Eligibility conditions** At least 3 border/coast guards from 3 different EU or AC (or at least 5 for the open sub-topic)
- **Deadline** 22 Aug 2019
- **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 while at the same time tackling irregular migration and enhancing our internal security

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-BES01-2018-2019-2020 - Scope

Human factors … of BES

- 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.

- Sub-topic: [2019] Open

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-BES02-2018-2019-2020

Technologies to enhance border and external security

- **Type of Action** Research & Innovation Action
- **Output TRL** 5 to 6
- **Project duration** not specified
- **Budget per project** ~7 M€
- **Total budget** 21 M€ in 2019

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

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

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-BES02-2018-2019-2020 - Scope

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
  - 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
  - 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: [2018-2019-2020] Open

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-BES03-EBCGA-2018-2019-2020

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 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 AC (or at least 5 for the open sub-topic)
  Consortia must be coordinated by a practitioner under civilian authority
- **Deadline** 22 Aug 2019
- **Challenge**
  - ❑ BES solutions at high TRL exist but they need to be demonstrated in the context of actual operations

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-BES03-EBCGA-2018-2019-2020 - Scope

Demonstration of applied solutions to enhance BES

- 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 maritime incidents, and a reduction in the death toll at sea.

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

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-GM

General Matters

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-GM01-2018-2019-2020

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** 3,5 M€ in 2019

- **Eligibility conditions** - At least 8 practitioners from 8 different EU or associated countries
  - 25% of cost to interact with industry and academia

- **Deadline** 22 Aug 2019

- **Challenge**
  - ❑ Practitioners interested in the uptake of security research and innovation are dedicated to performing their duty and are focused on their tasks.

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-GM01-2018-2019-2020 - Scope

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 the specific area of specialisation:

the handling of hybrid threats.

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-DS

Digital Security
Cybersecurity and Digital Privacy

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-DS03-2019-2020

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
- **Deadline** 22 Aug 2019
- **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

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-DS03-2019-2020 - Scope

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.

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-DS05-2018-2019 (1/3)

Digital security, privacy and accountability in critical sectors

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

- **Type of Action** Innovation Action
- **Output TRL** 7
- **Budget per project** 5 M€
- **Total budget** 10 M
- **Deadline** 22 Aug 2019

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

- **Type of Action** Research & Innovation Action
- **Output TRL** 7
- **Budget per project** 5 M€
- **Total budget** 10 M
- **Deadline** 22 Aug 2019

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

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-DS05-2018-2019 - Scope (2/3)

Digital security, privacy and accountability in critical sectors

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

Proposals under this sub-topic should tackle on at least two of the following items:

1. Secure access management for citizens to all types of vehicles. Novel tailored approaches related to cybersecurity by design in transportation systems
2. Assurance and protection against specific cyber-attacks in the multimodal transport domain, addressing interconnected threats and propagated vulnerabilities. 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).
3. Standardization to allow the quick adoption of cybersecurity best practices in the domain. Evaluate the feasibility of a security labelling for transportation.

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-DS05-2018-2019 - Scope (3/3)

Digital security, privacy and accountability in critical sectors

Sub-topic b [2019]: Digital security, privacy and personal data protection in **healthcare ecosystem**

Proposals under this sub-topic should tackle on at least two of the following items:

1. In collaboration with all stakeholders in the healthcare ecosystem and CERTs/CSIRTs, develop dynamic vulnerability data basis for collecting, uploading, maintaining, and disseminating vulnerabilities of ICT-based medical systems, technologies, applications and services. Build dynamic taxonomies for medical-related attacks in order to become the basis for building healthcare cybersecurity incident management systems.
2. Deliver dynamic, evidence-based, sophisticated security, privacy and personal data protection risk assessment frameworks and tools that can deal with cascading effects of threats, (compliant with appropriate cybersecurity standards e.g. ISO27001, ISO27005, ISO28000).
3. Provide collaborative privacy-aware tools enabling healthcare stakeholders to access and share information.

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-ICT & ICT

Cybersecurity in ICT

Co-funded by the Horizon 2020
Framework Programme of the European Union

SU-ICT-02-2020
Building blocks for resilience in evolving ICT systems

- Scope:

  At least one of the following:
  - *Cybersecurity/privacy audit, certification and standardisation*
  - *Trusted supply chains of ICT systems*
  - *Designing and developing privacy-friendly and secure software and hardware*

Deadline: novembre 2019

Type	Output TRL	Budget/proj. (M€)	Total Budget total (2020)
RIA	5	4-5	47 M€

Co-funded by the Horizon 2020
Framework Programme of the European Union

WP Features 2019-2020:

Cross-cutting issues – where is it flagged?

Call	Topic #		ToA	SSH	Gender	Int. Coop
INFRA	INFRA	01	IA			X
		02	IA	X		
SEC	BES	01	RIA	X	X	X
		02	RIA			
		03	IA			
	DRS	01	RIA	X	X	X
		02	RIA	X	X	X
		03	IA			
		04	RIA			
		05	IA			
	FCT	01	RIA	X	X	
		02	RIA	X		
		03	IA	X		
	GM	01	CSA			
		02	CSA			
DS	DS	03	IA	X		
		05	RIA/IA	X		

Co-funded by the Horizon 2020
Framework Programme of the European Union