EN

Annex 17

Horizon 2020

Work Programme 2018-2020

14. Secure societies - Protecting freedom and security of Europe and its citizens

Table of contents

Introduction

Horizon 2020 Interim Evaluation

This work programme part takes account of the results of the Interim Evaluation of Horizon 2020. The approach taken in the 2016-2017 work programme of requiring a minimum number of practitioners in a consortium is continued. This not only ensures that the research projects are attuned to the requirements of practitioners, but also reduces oversubscription. The involvement of SMEs is promoted including by introducing a topic requiring the coordinator to be an SME. Furthermore, the need to bring newly-developed technologies closer to the market is promoted through the application of Pre-Commercial Procurements. It should be noted that security research is challenge-driven; its main purpose is to develop new technologies and working methods that will help practitioners respond to emerging security threats. As a consequence, TRL levels in this work programme part are relatively high.

Open access to research data

Please note that grant beneficiaries under Horizon 2020 will engage in research data sharing by default, as stipulated in Article 29.3 of the Horizon 2020 Model Grant Agreement (including the creation of Data Management Plan). However, keeping in mind that all proposals under this work programme part will be subject to Security Scrutiny, the attention of the grant beneficiaries of this work programme part is drawn to the fact that they may find more appropriate to opt out of these arrangements. More information can be found under General Annex L of the work programme.

Societal aspects

Security as societal value is a guiding principle throughout this work programme part. All individual actions must be in compliance with the provisions of the Charter of Fundamental Rights of the European Union.[1]. When dealing with the development of technologies, it is recommended that actions consider the concepts of "privacy by design", "data protection by design", "privacy by default", and "data protection by default".

A 'Societal Impact Table' is a specific feature of this work programme part. The table puts an emphasis on societal aspects of security research. It checks whether the proposed security research meets the needs of and benefits society and does not have negative impacts on society. Applicants must fill in the 'Societal Impact Table' as part of the submission process. This table is taken into account during the evaluation under the 'Impact' criteria.

Responsible Research and Innovation[2]

The calls under 'Secure societies – Protecting freedom and security of Europe and its citizens' are in line with the Horizon 2020 Responsible Research and Innovation (RRI) cross-cutting

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF

[2] http://ec.europa.eu/research/swafs/pdf/rome_declaration_RRI_final_21_November.pdf

issue, engaging society on sensitive security issues, integrating the gender and ethical dimensions, ensuring the access to security research outcomes whenever possible and encouraging formal and informal science education relating to security. Activities will be multi-actor and underpinned by public engagement.

Sustainable Development Goals

The actions are expected to support Europe's endeavours to implement the Sustainable Development Goals (SDGs), particularly SDG 16 'Promote just, peaceful and inclusive societies'. Specific actions may also contribute to other SDGs such as SDG 11 'Make cities and human settlements inclusive, safe, resilient and sustainable'.

Possible synergies with defence research

Following up the EU Global Strategy in the security and defence area, the Commission adopted the European Defence Action Plan (EDAP)[3] followed by a Communication on the establishment of a European Defence Fund with two windows to support collaborative defence research (research window) and defence capability development programmes (capability window). The defence research window is already operational with funding opportunities under the Pilot Project and the launch of the Preparatory Action on Defence Research with the publication of a first call for proposals on 7 June 2017. As a first step in the implementation of the capability window the Commission put forward a proposal for a European defence industrial development programme under the current MFF from 2019-2020. Whereas activities under Horizon 2020 will have an exclusive focus on civil applications, coordination with the activities of the European Defence Agency (EDA) may be considered with possible synergies being established with projects funded by the EDA programmes[4]. Where necessary, actions should clearly demonstrate how they complement and do not overlap with actions undertaken under the Preparatory Action on Defence Research.

Focus Area 'Boosting the effectiveness of the Security Union'

All actions under this work programme part contribute to the Focus Area 'Boosting the effectiveness of the Security Union' (see below).

Contribution to focus area(s)

Focus Area 'Boosting the effectiveness of the Security Union' (SU): EUR 704.59 million

[3] COM(2016)950.

[4] http://eda.europa.eu/what-we-do/eda-priorities/research-technology

Boosting the effectiveness of the Security Union - Focus Area

Working to ensure a high level of security for Europeans is an objective set by the Treaties, and a common European responsibility. The importance of the Security Union agenda has been highlighted in the Commission Communication of 20 April 2016[5] and by the subsequent appointment of a Commissioner for the Security Union. The majority of Member States depend entirely on Horizon 2020 to cover their needs for innovative security solutions, and it represents 50% of the overall public funding for security research in the EU.

At the core of research in this area is the development of new products to meet the needs of security practitioners. Research is not just about developing new technologies or applying emerging technologies, but also requires understanding phenomena such as violent radicalisation and the development of more effective policies and interventions. This means social sciences and the humanities will be involved.

To help end results correspond to real needs, research will generally require the involvement of security practitioners and those working with at-risk groups, for example fire and rescue services, police forces, border and coast guards, municipalities, social workers, educators and civil society actors. One challenge is segmentation of civil security industry largely into national markets. Progressive development of a single market also in this area can be expected to bring benefits of economies of scale, providing incentives to businesses to develop new solutions and lowering costs for purchasers. To facilitate supply and demand for new goods and services, innovative procurement (PCP, PPI) will be used.

The Focus Area will support implementation of the Security Union priorities: reacting to and recovering from natural and man-made disasters; preventing, investigating and prosecuting crime including organised crime and terrorism; improving border entry security; protecting infrastructure against natural and man-made threats, including cyber-attacks; digital security, privacy and data protection; and space-related research.

Focus area impacts:

- Reduced loss of life and reduced environmental, material and economic losses from natural and man-made disasters.
- Key infrastructure better protected against natural and man-made threats, including cyber-attacks.
- New products that meet the needs of security practitioners in the EU, including for investigating and prosecuting crime (including cybercrime) and terrorism.
- EU borders better secured against the entry of undesirable persons or goods.

[5] *Delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union*, COM(2016) 230 final, 20.4.2016.

- Ensuring a secure and trusted networked environment for the governments, businesses and individuals, thus positioning the EU as a world leader in building a more secure digital economy.

- Support for EU and national policies related to security, including those focusing on prevention.

- Space-related research harnessed to support security.

- Better understanding of the complex and interrelated drivers and societal contexts of security challenges including in particular radicalisation and polarisation.

Components of the focus area, whose topics are identified as SU-xxx in the Horizon 2020 work programme, include actions from the LEIT-ICT, LEIT-Space and Societal Challenges 1, 3, 6 and 7. In addition, related activities are financed by other parts of the Horizon 2020 work programme including the European Research Council (ERC), the SME instrument, the SESAR Joint Undertaking and the ECSEL Joint Undertaking.

Call - Protecting the infrastructure of Europe and the people in the European smart cities[6]

H2020-SU-INFRA-2018-2019-2020

Threats against crowded areas and disruptions in the operation of our countries' infrastructure may limit the liberties of our citizens and put at risk the functioning of our societies and their economies. The security and resilience of Europe critical infrastructure needs to be ensured because disruptions in their operations may entail the collapse of large sectors of our activities. Threats to soft targets such as crowded areas may have less long-term physical impact, but may be highly damaging due to potentially large numbers of victims and subsequent psychological and sociological impacts.

The topics below in this Call "Protecting the infrastructure in Europe" are part of the contribution of the Commission to the Cybersecurity contractual Public Private Partnership (cPPP), established in July 2016. This cPPP will facilitate the engagement of end-user operators in sectors that are important beneficiaries and customers of cybersecurity solutions towards defining and providing to the industry their sector-specific digital security, privacy and personal data protection common requirements.

When a topic has eligibility and admissibility conditions which require the active involvement of specific entities (e.g.: operators), this means that these entities have to be participants and should be directly involved in the carrying out of the tasks foreseen in the grant. When a reference is made to "practitioners", the text refers to someone who is qualified or registered to practice a particular occupation, profession in the field of security or civil protection. Applicants should identify clearly which members of the consortium they consider "practitioners" in the specific context of their proposal, and to include a clear description of their respective role and added-value as practitioners in section 4.3 of proposal part B4-6.

Whereas activities will have an exclusive focus on civil applications, coordination with the activities of the European Defence Agency (EDA) may be considered with possible synergies being established with projects funded by the EDA programmes[7]. The complementarity of such synergies should be described comprehensively. On-going cooperation should be taken into account. Only an explicit and firm commitment from EDA-funded projects to contribute to a project may positively impact the evaluation of a proposal submitted under this work programme part.

In this Call, "standards" and "standardisation" are used in a broad sense, except where they are specifically referred to as "European standards" or "European standardisation".

All topics in this work programme part will be subject to security scrutiny.

---

[6] The Commission reserves the possibility under this call to exclude a specific project from the delegation to the REA if it appears that that project would necessarily have a close link to the development of EU policies in the field of security.

[7] http://eda.europa.eu/what-we-do/eda-priorities/research-technology

The aim of this Call is to protect and improve the resilience of critical infrastructures and soft targets.

Proposals are invited against the following topic(s):

SU-INFRA01-2018-2019-2020: Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe[8]

Specific Challenge: Disruptions in the operation of our countries' critical infrastructure may result from many kinds of hazards and physical and/or cyber-attacks on installations and their interconnected systems. Recent events demonstrate the increase of combined physical and cyber-attacks due to their interdependencies. A comprehensive, yet installation-specific, approach is needed to secure existing or future, public or private, connected and interdependent installations, plants and systems. Budgetary constraints on both the public and private sectors mean that new security solutions must be more accurate, efficient and cost-effective, and possibly more automated than the ones currently available.

Scope: Proposals should cover: forecast, assessment of physical and cyber risks, prevention, detection, response, and in case of failure, mitigation of consequences (including novel installation designs), and fast recovery after incidents, over the life span of the infrastructure, with a view to achieving the security and resilience of all functions performed by the installations, and of neighbouring populations and the environment.

They should:

(a) assess in detail all aspects of interdependent physical (e.g. bombing, sabotage and attacks with a variety of weapons against installations, buildings and ships; plane or drone overflights and crashes; spreading of fires, floods, landslides, disastrous consequences of global warming, seismic activity, space weather, combined threats, etc.) and cyber threats and incidents (e.g. malfunction of SCADA system, non-authorised access of server, electronic interference, distributed attacks), and 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 and by comparing the results with other risk assessment methodologies,

(c) develop improved real-time, evidence-based security management of physical and cyber threats, taking account of the ageing of existing infrastructure, and

(d) provide scenarios and recommendations for policy planning, engagement of the civil society, and investment measures encompassing all aspects of prevention-detection-response-mitigation

Innovative methods should be proposed for sharing information with the public in the vicinity of the installations - including through social media and with the involvement of civil society

[8] It is expected that this topic will continue in 2020.

organisations -, for the protection of first responders such as rescue teams, security teams and monitoring teams, and for ensuring service continuity.

In 2018 and 2019, they should focus on any type of installation belonging to one of the following critical infrastructures: water systems, energy infrastructure (power plants and distribution, oil rigs, offshore platforms), transport infrastructure (airports, ports, railways, urban multimodal nodes), communication infrastructures and ground segments of space systems, health services, e-commerce and the postal infrastructure, sensitive industrial sites and plants, and financial services. Priorities for 2020 will be defined at a later stage. When selecting for funding the proposals submitted in 2018 or 2019, the Commission will take due account of similar projects financed in the previous years since 2016, with a view to cover the largest possible spectrum of installations. Each year, a list of infrastructures excluded from the Call will be published on the participant portal.

Consortia should involve the largest variety of relevant beneficiaries, including infrastructure owners and operators, first responders, industry, technologists and social scientists, etc. The participation of SMEs is strongly encouraged.

In line with the EU's strategy for international cooperation in research and innovation[9] international cooperation is encouraged, and in particular with international research partners in the context of the International Forum to Advance First Responder Innovation[10] in which the Commission has decided to participate.

The centre of gravity for technology development with actions funded under this topic is expected to be up to TRL 7 – see General Annex G of the Horizon 2020 Work Programme.

Indicative budget: The Commission considers that proposals requesting a contribution from the EU of about EUR 7 to 8 million would allow this topic to be addressed appropriately. Nonetheless this does not preclude the submission and selection of proposals requesting other amounts

Expected Impact: Short term:

- State-of-the-art analysis of physical/cyber detection technologies and risk scenarios, in the context of a specific critical infrastructure.
- Analysis of both physical and cyber vulnerabilities of a specific critical infrastructure, including the combination of both real situation awareness and cyber situation awareness within the environment of the infrastructure.
- In situ demonstrations of efficient and cost-effective solutions to the largest audience, beyond the project participants.

Medium term

[9] COM(2012) 497.

[10] http://www.internationalresponderforum.org/

- Innovative (novel or improved), integrated, and incremental solutions to prevent, detect, respond and mitigate physical and cyber threats to a specific Critical Infrastructure.
- Innovative approaches to monitoring the environment, to protecting and communicating with the inhabitants in the vicinity of the critical infrastructure.
- Security risk management plans integrating systemic and both physical and cyber aspects.
- Tools, concepts, and technologies for combatting both physical and cyber threats to a specific critical infrastructure.
- Where relevant, test beds for industrial automation and control system for critical infrastructure in Europe, to measure the performance of critical infrastructure systems, when equipped with cyber and physical security protective measures, against prevailing standards and guidelines.
- Test results and validation of models for the protection of a specific critical infrastructure against physical and cyber threats.
- Establishment and dissemination throughout the relevant user communities of specific models for information sharing on incidents, threats and vulnerabilities with respect to both physical and cyber threats.

Long term

- Convergence of safety and security standards, and the pre-establishment of certification mechanisms.
- Secure, interoperable interfaces among different critical infrastructures to prevent from cascading effects.
- Contributions to relevant sectorial frameworks or regulatory initiatives.

Type of Action: Innovation action

The conditions related to this topic are provided at the end of this call and in the General Annexes.

SU-INFRA02-2019: Security for smart and safe cities, including for public spaces[11]

Specific Challenge: In the cities, public spaces such as malls, open crowded gathering areas and events, and non-restricted areas of transport infrastructures, constitute "soft targets", that is potential, numerous targets spread across the urban area and subject to "low cost" attacks strongly impacting the citizens. The generation, processing and sharing of large quantities of data in smart cities make urban systems and services potentially more responsive, and able to

[11] This topic complements other smart cities actions, including those under the European Innovation Partnership on Smart Cities and Communities.

act upon real-time data. On the one hand, smart cities provide for improving the security of open and crowded areas against threats (incl. terrorist threats) and risks, by leveraging wide networks of detection and prevention capabilities that can be combined with human response to crisis to enhance first responders' actions. On the other hand, the distinct smart technological and communication environments (urban, transport infrastructures, companies, industry) within a smart city require a common cybersecurity management approach.

Scope: The security and good operation of a smart and safe city relies on interconnected, complex and interdependent networks and systems: public transportation networks, energy, communication, transactional infrastructure, civil security and law enforcement agencies, road traffic, public interest networks and services.

Such networks provide with an efficient infrastructure for detection resources and "big data" collection. The screening of such data are being used by security practitioners to enhance their capabilities and performances. For instance, crowd protection and the security of public and government buildings can be improved through the identification of threats or of crime perpetrators, and the early detection of dangerous devices or products; first responders may get quicker on site by calculating in real time the shorter possible route to the scene of disaster.

Proposals under this topic should 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. The proposed pilots should 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

In designing the platform, proposals should:

- involve actively the security actors of the city area, their coordination and governance;
- solve interoperability issues, and ensure the interconnection and integration of the city smart systems with the systems supporting the security practitioners locally, including through modelling and simulating their interdependence;
- enhance the security of city smart systems, notably in terms of access control (e.g. with digital security measures such as layered authentication and access), secure communication and data storage, and address their possible misuse by criminals;
- consider new concepts of operation resulting from novel monitoring methods, data provided by extensive networks of sensors and social media;

- consider mitigation strategies in the context of a variety of scenarios in order 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 for the sharing, consolidation and analysis of multi-sourced data.

The proposals should also address at least one of the following key issues:

- Simulation, detection and analysis of the additional security threats and risks created through the interconnection of smart systems (e.g. Internet of Things (IoT), in particular those IoT objects used by security practitioners) and smart infrastructures (e.g. smart (government) buildings, smart railways, smart ports, smart factories, smart bridges, smart hospitals, large gathering of people in smart infrastructure) within a smart city;
- Delivery of a cyber-security framework to ease collaboration across all smart cities stakeholders, from urban planners to infrastructure operators, security practitioners, IT supervisors and providers across smart organizations within the city;
- Support and implementation of a common approach to securing and managing in a reliable and untamperable manner the data from all the smart infrastructures and systems hosted in a smart city supporting the citizens, the public authorities, the security practitioners, and the urban economy in creating transparent, efficient, accountable cyber-secure data-handling processes, in line with data protection legislation.

Digital security awareness should be integrated into the eco-system of humans, competences, services and solutions which should be able to adapt rapidly to the evolutions of cyber-threats or even to surpass them.

The centre of gravity for technology development with actions funded under this topic is expected to be up to TRL 7 – see General Annex G of the Horizon 2020 Work Programme.

Solutions are to be developed in compliance with fundamental rights, privacy and data protection, especially as the development of big data creates specific challenges. Therefore, full compliance with data protection legislations must be ensured in exploiting big data. Societal aspects (e.g. perception of security, possible effects of technological solutions on societal resilience) have to be taken into account in a comprehensive and thorough manner.

Projects should also foresee activities and envisage resources for cooperating with other projects funded under this topic and with other relevant projects in the field funded by Horizon 2020.

The Commission considers that proposals requesting a contribution from the EU of about EUR 8 million would allow this specific challenge to be addressed appropriately.

Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected Impact:

- Creation of dedicated, harmonised, advance cybersecurity solutions for smart cities adopting common approaches with all involved stakeholders (e.g. administrators of smart city/port/transport) balancing their – sometimes conflicting – goals (e.g. urban development, efficiency, growth, competitiveness, resilience).
- In situ demonstrations of efficient and cost-effective solutions to the largest audience, beyond the project participants.
- An easier level of integration by developing a holistic cyber-security framework for smart cities that benefits all smart infrastructures hosted within it (e.g. smart buildings, smart ports, smart railways, smart logistics).
- IoT ecosystems (rather than distributed IoT infrastructures) built adopting common approaches in their cybersecurity management, achieving economies of scale (e.g. avoiding duplication of efforts in the analysis of IoT data, selection of cybersecurity controls).
- Novel concepts of operations taking account of mutiple, heterogeneous data sources and the social media.
- Novel tools and systemic approaches to protect citizens against threats to soft targets in a Smart City.

Type of Action: Innovation action

The conditions related to this topic are provided at the end of this call and in the General Annexes.

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

Opening date(s), deadline(s), indicative budget(s):[12]

[12] The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The deadline(s) in 2019 and 2020 are indicative and subject to separate financing decisions for 2019 and 2020.
The budget amounts for the 2018 budget are subject to the availability of the appropriations provided for in the draft budget for 2018 after the adoption of the budget 2018 by the budgetary authority or, if the budget is not adopted, as provided for in the system of provisional twelfths.
The budget amounts for the 2019 and 2020 budget are indicative and will be subject to separate financing decisions to cover the amounts to be allocated for 2019 and for 2020.

Topics (Type of Action)	Budgets (EUR million)			Deadlines
	2018	2019	2020	
Opening: 15 Mar 2018				
SU-INFRA01-2018-2019-2020 (IA)	24.00			23 Aug 2018
Opening: 14 Mar 2019				
SU-INFRA01-2018-2019-2020 (IA)		22.00		22 Aug 2019
SU-INFRA02-2019 (IA)		16.00		
Opening: To be defined				
Focus area topic(s) for 2020			18.00	To be defined
Overall indicative budget	24.00	38.00	18.00	

Indicative timetable for evaluation and grant agreement signature:

For single stage procedure:

- Information on the outcome of the evaluation: Maximum 5 months from the final date for submission; and
- Indicative date for the signing of grant agreements: Maximum 8 months from the final date for submission.

Eligibility and admissibility conditions: The conditions are described in General Annexes B and C of the work programme. The following exceptions apply:

SU-INFRA01-2018-2019-2020	At least 2 operators of the chosen type of critical infrastructure operating in 2 Member States or Associated Countries must be beneficiaries (possibly, but not necessarily: coordinator) of the grant agreement and should be directly involved in the carrying out of the tasks foreseen in the grant. The participation of industry able to provide security solutions is required. The duration of the proposed activities must not exceed 24 months.
SU-INFRA02-2019	At least the local governments of 2 cities or metropolitan areas in 2 Member States or Associated Countries must be beneficiaries (possibly, but not necessarily: coordinator) of the

	grant agreement and should be directly involved in the carrying out of the tasks foreseen in the grant. The participation of industry able to provide security solutions is required. The duration of the proposed activities must not exceed 24 months.

Evaluation criteria, scoring and threshold: The criteria, scoring and threshold are described in General Annex H of the work programme.

Evaluation Procedure: The procedure for setting a priority order for proposals with the same score is given in General Annex H of the work programme.

The full evaluation procedure is described in the relevant guide published on the Participant Portal.

Consortium agreement:

All topics of this call	Members of consortium are required to conclude a consortium agreement, in principle prior to the signature of the grant agreement.

Call - Security[13]

H2020-SU-SEC-2018-2019-2020

This Call deals with R&D and innovation towards establishing disaster-resilient societies, fighting against crime and terrorism, and improving border and external security.

When a topic has eligibility and admissibility conditions which require the active involvement of specific entities (e.g.: '3 Law Enforcement Agencies (LEA) from at least 3 different EU or Associated countries'), this means that these entities have to be participants and should be directly involved in the carrying out of the tasks foreseen in the grant. When a reference is made to "practitioners", the text refers to someone who is qualified or registered to practice a particular occupation, profession in the field of security or civil protection. Applicants should identify clearly which members of the consortium they consider "practitioners" in the specific context of their proposal, and to include a clear description of their respective role and added-value as practitioners in section 4.3 of proposal part B4-6.

Whereas activities will have an exclusive focus on civil applications, coordination with the activities of the European Defence Agency (EDA) may be considered with possible synergies being established with projects funded by the EDA programmes[14]. The complementarity of such synergies should be described comprehensively. On-going cooperation should be taken into account. Only an explicit and firm commitment from EDA-funded projects to contribute to a project may positively impact the evaluation of a proposal submitted under this work programme part.

In this Call, "standards" and "standardisation" are used in a broad sense, except where they are specifically referred to as "European standards" or "European standardisation".

All topics in this work programme part will be subject to security scrutiny.

Disaster-Resilient Societies

Securing itself against, and being prepared for, disasters is one of the central elements of the functioning of any society. There are hardly any societal functions which are not to some extent exposed to natural or man-made disasters and related resilience and security issues.

The aim of this section is to advance innovation in the society at large, and among first responders (as acknowledged within the International Forum to Advance First Responder Innovation[15] *in which the Commission has decided to participate) to reduce the loss of human life and to reduce environmental, economic and material damage from natural and man-made*

[13] The Commission reserves the possibility under this call to exclude a specific project from the delegation to the REA if it appears that that project would necessarily have a close link to the development of EU policies in the field of security.

[14] http://eda.europa.eu/what-we-do/eda-priorities/research-technology

[15] *http://www.internationalresponderforum.org/*

disasters, including from climate-related weather events, earthquakes and volcanic events, space weather events, industrial disasters, crime and terrorism threats.

Proposals are invited against the following topic(s):

SU-DRS01-2018-2019-2020: Human factors, and social, societal, and organisational aspects for disaster-resilient societies[16]

Specific Challenge: The resilience of societies heavily depends on how their citizens behave individually or collectively, and how governments and civil society organisations design and implement policies for mitigating risks, preparing for, reacting to, overcoming, and learning from disasters. The spread of new technologies and media are inducing dramatic changes in how individuals and communities behave, and they are affecting societies in unpredictable ways. Building the resilience of society and citizens requires a better understanding and implementation of these new technologies, media and tools, and their capacity to raise disaster risk awareness, to improve citizen understanding of risks, to build a culture of risks in society, to enable an effective response from affected populations, to improve functional organisation in most fragile and vulnerable environments, and to increase the resilience of health services, social services, education, and governance, in line with target (d) of the Sendai Framework on critical infrastructure and disruption of basic services.

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

Recent disasters related either to natural causes (including climate-related hazards) or to terrorist attacks have shown gaps in the level of preparedness of European society for disasters, and therefore highlighted the importance of increasing risk awareness, and hence resilience among people and decision-makers in Europe. There is much that can be learned from certain countries with a high level of risk of natural disasters (e.g. Japan with high-levels of risks of earthquakes, volcanic events, and tsunamis) and where risk awareness is high. Research is required with a view to how cultural changes among individuals, business managers, government officials, and communities can create a resilient society in Europe, in line with the Sendai Framework for Disaster Risk Reduction.

Over the past few years several ways to exploit social media and other crowd-sourced data in emergency situations have been studied, and some put in place, but their impacts are not well known. Research is needed to assess such practices for different disaster scenarios (natural hazards, industrial disasters, terrorist threats) involving different actors, including first responders, city authorities and citizens. Research should analyse both the positive and negative roles of social media and crowd-sourced data in crisis situations. For instance in the wake of a terror attack or natural disaster they offer a quick and easy way to relieve friends and family from worry (where networks are not down), and they generate valuable information about the affected area in the first moments after a disaster; they have been used to spread early warnings and important safety information. However, social media may also be used to spread false statements and to overstate threats, so the validation processes of

[16] It is expected that this topic will continue in 2020.

information should also be addressed. Social media itself is reliant upon the functioning of critical infrastructure such as phone networks and may not always be available. Research should also address solutions for communication between first responders and the victims and citizens in the affected area.

Research on risk awareness should encompass the whole of the disaster management cycle, from prevention (e.g. through education) and preparedness (knowing how to react), emergency management (collaboration and communication before and during an event), response (empowering citizens to act efficiently by themselves according to more effective practices and following established guidelines), and recovery (knowledge to build back better). Researchers should take into account tangible and intangible cultural heritage, traditional know-how, land use, construction technologies, and other local knowledge which is a valuable source of information for the local communities and can help prevent the creation of new risks, to reduce existing risks, to prepare for and to respond to disasters and to build back better.

Sub-issues to be addressed are diversity in risk perception (as a result of e.g. geography (within Europe), attitudes, institutional and social trust, gender and socio-economic contexts), in vulnerabilities and in understanding responses to crises in order to propose new approaches and strategies for community awareness, for leadership, and for crisis readiness and management with a particular emphasis on the use of new technologies.

For achieving disaster-resilient societies that cope with disasters and build back better, the research community needs to transfer research outputs in an appropriate manner to meet citizen expectations given the current levels of risk acceptance, risk awareness, and involvement of civil society organisations in a mediating role.

Civil society organisations, first responders, (national, regional, local, and city) authorities are invited to propose strategies, processes, and methods to enable citizens better to access research results related to disaster resilience, and to prepare the ground for exercises involving citizens. These strategies, processes, and methods should be tested with citizens and communities representative of European diversity and for different types of disaster, in particular with regards to citizens' individual capacities and their involvement in checking and validating proposed tools, technologies and processes for disaster management. Studies will assess the value of raising awareness about relevant research among citizens and communities.

Proposals should be submitted by consortia involving relevant security practitioners and civil society organisations. Research should contribute to the understanding of society's awareness to risks in Europe in order to provide recommendations for the development of a culture of improved preparedness, adaptability, and resilience to risks, including the use of social media and crowd-sourced data, and the involvement of the citizens in the investigations and possible validation of tools and methods.

In line with the objectives of the Union's strategy for international cooperation in research and innovation (COM(2012)497), international cooperation according to the current rules of participation is encouraged (but not mandatory).

The Commission considers that proposals requesting a contribution from the EU of about EUR 5 million would allow this specific challenge to be addressed appropriately through multidisciplinary projects confronting different schools of thoughts. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected Impact: As a result of this action, Member States and Regional authorities as well as City and Metropolitan authorities should benefit from recommendations and tools aimed at improving the adaptability and preparedness of societies to different disaster risks, including:

- Comparative analysis of the European diversity in terms of risk-perception amongst citizens, and of vulnerabilities;
- Comparative analysis of different approaches to adapt to, and be prepared for risks in different countries (both within and outside the European Union), and among communities in precarious socio-economic conditions;
- Advances through the cross-fertilisation of concepts resulting from the collision of different ways of thinking and of different approaches developed by various partners in the proposals;
- Identification of existing tools and guidelines for an improved prevention (including risk understanding and communication), preparedness (including training involving citizens), alert systems and their recognition by citizens, responses using citizen's competencies and local knowledge, and recovery;
- Improved information exchanges among different actors involved, including first responders, local authorities, schools, and citizen representatives;
- Field-validation of different approaches related to different disaster risks involving the above actors, in representative urban and non-urban environments, including in areas where precarious socio-economic conditions prevail;
- Intensive sharing, among communities, of good practices and of learnings resulting from citizen-scientist interaction;
- A consolidated, common European understanding of disaster resilience.

Type of Action: Research and Innovation action

The conditions related to this topic are provided at the end of this call and in the General Annexes.

SU-DRS02-2018-2019-2020: Technologies for first responders[17]

Specific Challenge: Resilience is critical to allow authorities to take proper measures in response to severe disasters, both natural (including climate-related extreme events) and man-made. Innovation for disaster-resilient societies may draw from novel technologies, provided that they are affordable, accepted by the citizens, and customized and implemented for the (cross-sectoral) needs of first responders.

Scope: Proposals are invited to propose novel solutions improving the protection of first responders against multiple and unexpected dangers, or enhancing their capacities by addressing related research and innovation issues, in particular:

- Sub-topic 1: [2018] Victim-detection technologies

The quick detection of victims potentially trapped in buildings as a result of all sorts of disasters of natural, accidental, or man-made or of terrorist origins is a major issue for first responders. Novel technologies should enable them to save the time taken to detect victims who are not visible, enabling more efficient and faster rescue operations leading to higher chances of saving lives and reducing injuries.

- Sub-topic 2: [2019] Innovation for rapid and accurate pathogens detection

Novel technologies are required by first responders for the rapid and accurate detection of pathogens, as well as tools for joint epidemiological and criminal risk and threat assessment and investigation.

- Sub-topic 3: [2020] Methods and guidelines for pre-hospital life support and triage

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

Other technologies for use by first responders may be subject of proposals provided that they involve a large number of first responders' organisations (see eligibility and admissibility conditions.) For instance, but not exclusively: communicating and smart wearables for first responders and K9 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.

Any novel technology or methodology under this topic should be tested and validated, not just in laboratories but also in training installations and through in-situ experimental deployment. They therefore need to be quick to deploy, bases on resilient and robust communication infrastructure. First responders, including through interdisciplinary teams (e.g. involving medical emergency services, public health authorities, law enforcement team, civil protection

[17] It is expected that this topic will continue in 2020.

professionals, etc.) need to be involved in these activities. Proposals should address the participation of first responders in a systematic manner, and propose new methods on how to involve them and to organise their interaction with researchers when developing, testing, and validating technologies and methods.

Solutions are to be developed in compliance with European societal values, fundamental rights and applicable legislation, including in the area of privacy, personal data protection and free movement of persons. Societal aspects (e.g. perception of security, possible effects of technological solutions on societal resilience, gender diversity) have to be taken into account in a comprehensive and thorough manner.

In line with the objectives of the Union's strategy for international cooperation in research and innovation (COM(2012)497), international cooperation according to the current rules of participation is encouraged (but not mandatory), in particular with Japanese or Korean research centres. Co-funding opportunities from the Japan Science and Technology Agency exist for Japanese partners. For more information, please consult http://www.jst.go.jp/sicp/announce_eujoint_04_GeneralInfo.html. Co-funding opportunities from the Korean MSIP/NRF exist for Korean partners. For more information on Korea, please consult http://www.nrf.re.kr/eng/main and http://www.nrf.re.kr/biz/info/notice/view?nts_no=82388&biz_no=116&search_type=ALL&search_keyword=EU&page=.

The centre of gravity for technology development with actions funded under this topic is expected to be up to TRL 4 to 6 – see General Annex G of the Horizon 2020 Work Programme.

The Commission considers that proposals requesting a contribution from the EU of about EUR 7 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected Impact: As a result of this action, first responders should benefit from:

- Novel tools, technologies, guidelines and methods aimed at facilitating their operations
- New knowledge about field-validation of different tools, technologies and approaches involving first responders in (real-life) scenarios

Type of Action: Research and Innovation action

The conditions related to this topic are provided at the end of this call and in the General Annexes.

SU-DRS03-2018-2019-2020: Pre-normative research and demonstration for disaster-resilient societies[18]

Specific Challenge: A reason for the difficult interaction among practitioners, and for the low levels of interoperability of equipment and procedures implemented by first responders, lies in there being insufficient harmonisation and standardisation, which pre-normative research and demonstrations may address effectively.

The security market in Europe is an institutional market that is highly fragmented (because of the lack of standardization and harmonised certification), and with a strong societal dimension (it directly affects in many ways the citizens). In this context, the Mandate M/487 to Establish Security Standards coordinated by the European Committee for Standardization has clearly recognized the whole field of "crisis management and civil protection" as one of the three priorities for establishing standards in the security sector. It has identified the need for crisis management and civil protection standardization activities to facilitate response, effectiveness, efficiency and cooperation as top priorities, especially in what regards to natural hazard emergencies.

Scope: Proposals are invited to address issues related to pre-standardisation, in particular:

- Sub-topic 1: [2018] Pre-standardisation for the security of water supply

For several years research actions have led to the development of detection technologies to analyse drinking water. Based on the legacy of FP7-funded actions, clearer strategies to integrate current technologies in the existing water safety network should be designed. Testing facilities should interconnect the safety- and security-related networks of sensors that are deployed among water supply and distribution networks. The focus of action should be on networking testing facilities developed by water utilities to 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.

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

Generally speaking, the development of standards for civil protection in the areas of crisis management (including for systems, tools and services related to natural hazard and CBRN-E emergencies) will increase interoperability of equipment and procedures. Innovation actions should bring validated and positively-assessed practices into standards within or outside current standardisation processes. The involvement of well-established standardisation organisations is required. The complementarity of the proposed activities with activities supported by the European Defence Agency (EDA) in the CBRN-E area should be described comprehensively.

- Sub-topic 3: [2020] First aids vehicles deployment, training, maintenance, logistic and remote centralized coordination means

[18] It is expected that this topic will continue in 2020.

The centre of gravity for technology development with actions funded under this topic is expected to be up to TRL 6 to 7 – see General Annex G of the Horizon 2020 Work Programme.

The Commission considers that proposals requesting a contribution from the EU of about EUR 6 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected Impact: Medium term:

- [2018] full awareness of water supply facilities about the necessity of designing monitoring networks capable of detecting both contamination risks (safety) and deliberate poisoning (security);
- [2019] standards for interoperable equipment and procedures in the area of crisis management and civil protection (including natural hazard and CBRN-E emergencies in support to operations involving international crews;
- [2020] standards for an effective deployment of resources to respond to major crisis.

Type of Action: Innovation action

The conditions related to this topic are provided at the end of this call and in the General Annexes.

SU-DRS04-2019-2020: Chemical, biological, radiological and nuclear (CBRN) cluster[19]

Specific Challenge: Technologies and innovations in the field of CBRN are developed by companies which often face difficulties in bringing them to markets. At least three reasons may be identified:

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

In this context a platform has been established further to the response to topic SEC-05-DRS-2016-2017 in 2016. A larger number of innovative technologies, devices and services need to be added to this platform.

Scope: In 2019 and 2020 the Commission will select several RIAs aiming at research and development of novel CBRN technologies and innovations identified in the catalogue that is

[19] It is expected that this topic will continue in 2020.

updated by the ENCIRCLE project on a regular basis. Each of these actions will be led by an SME. Each consortium implementing such a RIA must not only establish a consortium agreement among its members, but also an agreement with the participants in the ENCIRCLE project which must settle how the results from the RIA will be exploited and integrated into platforms managed by ENCIRCLE.

Where applicable, the complementarity of the proposed activities with activities supported by the European Defence Agency (EDA) should be described comprehensively.

The centre of gravity for technology development with actions funded under this topic is expected to be up to TRL 4 to 6 – see General Annex G of the Horizon 2020 Work Programme.

Indicative budget: The Commission considers that proposals requesting a contribution from the EU of about EUR 3.5 million per action for this topic to be addressed appropriately. Nonetheless this does not preclude submission and selection of proposals requesting other amounts.

The following options of the Model Grant Agreement will be implemented:

- Option 1 of Article 41.3 of the Model Grant Agreement will be applied.
- *Grants awarded under* this topic *will be complementary to the grant agreement under* **SEC-05-DRS-05-2016-2017 part a)**. *The respective options of Article 2, Article 31.6 and Article 41.4 of the Model Grant Agreement*[20] *will be applied.*

Expected Impact:

- Shorter time to market for novel CBRN technologies and innovations
- More business deals leading to industrial products of interest to more practitioners in Europe (and world-wide).

Type of Action: Research and Innovation action

The conditions related to this topic are provided at the end of this call and in the General Annexes.

SU-DRS05-2019: Demonstration of novel concepts for the management of pandemic crises

Specific Challenge: Large-scale pandemics constitute an ever growing threat in today's globalized society, given the increasing flows of goods and people among continents. This challenge ought to be addressed internationally, and with the involvement of a large variety of practitioners and stakeholders, from planners in national health systems, to first responders. The Horizon 2020 work programme separately includes an EIC Horizon Prize for 'Early

[20] *http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/amga/h2020-amga_en.pdf*

Warning for Epidemics' that is relevant for preparedness and response specifically to vector-borne disease outbreaks.

Scope: In 2014 an exploratory phase was called for (in DRS4 of the 2014 Call in Societal Challenge 7) to address 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. It has also proposed innovative concepts to integrate better the existing tools and systems for health and security protection in case of large-scale pandemics, taking into account potential impacts of climate change.

All these recommendations and proposals will be made public on the portal of the Call in due time.

Demonstrations are now required to assess these novel concepts, in support of cross-border emergency approaches (phase 2), to strengthen preparedness and response to pandemics (including the detection of disease outbreaks that could lead to pandemics), in line with Decision 1082/2013/EU on serious cross-border threats to health[21] and the International Health Regulations (WHO, 2005)[22].

The Commission considers that proposals requesting a contribution from the EU of about EUR 10 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected Impact: Short term:

- Novel concepts for health and security protection in the case of large-scale pandemics, validated by international organisations and a large number of EU Member States including a commitment to sharing these novel concepts.
- A prototype IT system integrating innovative tools, and supporting existing emergency frameworks.
- An operational strategy for implementation of the concepts and IT system supporting cross-border preparedness and crisis management, and demonstrated in situ.

Type of Action: Innovation action

The conditions related to this topic are provided at the end of this call and in the General Annexes.

[21] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013D1082

[22] http://www.who.int/topics/international_health_regulations/en/

Fight against Crime and Terrorism

The ambition of the activities under "Fight against Crime and Terrorism" is to mitigate potential consequences of crime- and/or terrorism-related incidents or to avoid them. To this end, new technologies and capabilities are required. They should address the fight against and the prevention of crime (including cyber-crime), illegal trafficking and terrorism (including cyber-terrorism and CBRN-E attacks), along with understanding and tackling terrorist ideas and beliefs. Human factors and the societal context should be taken into account, whilst respecting fundamental rights, including privacy, protection of personal data and the free movement of persons.

Proposals are invited against the following topic(s):

SU-FCT01-2018-2019-2020: Human factors, and social, societal, and organisational aspects to solve issues in fighting against crime and terrorism[23]

Specific Challenge: The free and democratic EU society, based on the rule of law, mobility across national borders, globalised communication and finance infrastructure, provides many opportunities to its people. However, the benefits come along with risks related to crime and terrorism, a significant number of which have cross-border impacts within the EU. 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. The consistent efforts made by EU Member States and the EU to that effect are not enough, especially when criminal groups and their activities extend far beyond national borders.

Scope: The Lisbon Treaty enables the EU to act to develop itself as an area of freedom, security and justice. The EU Security Union is now in the building, and requires an EU-wide approach to security that integrates prevention, investigation and mitigation capabilities in the area of the fight against crime.

The globalisation of communications and finance infrastructure allows crime to develop and take new forms. Trafficking in human beings for all forms of exploitation purposes is a serious and organised crime often with cross-border dimension, violating fundamental rights of the individuals and creating a security challenge. Prevention of child sexual abuse and exploitation is another area where research is acutely needed. The use of the internet as a platform for child sex offenders to communicate, store and share child sexual exploitation material and to hunt for new victims continues to be one of the internet's most abhorrent aspects. Cybercriminality, as a whole, is not satisfactorily understood nor properly addressed; the constantly expanding attack surface combined with the ever increasing number of attack vectors requires a more structured approach. Radicalisation is yet another challenge of our society that requires a multi-disciplinary approach, with policy recommendations and practical solutions to be implemented by a variety of policy-makers and practitioners.

[23] It is expected that this topic will continue in 2020.

Proposed approaches need to rely on existing knowledge and to exclude approaches that have previously failed. The societal dimension of fight against crime and terrorism should be at the core of the proposed activities. Proposals should be submitted by consortia involving relevant security practitioners and civil society organisations, each under only one of the following sub-topics:

- **Sub-topic 1: [2018] New methods to prevent, investigate and mitigate trafficking of human beings and child sexual exploitation – and on the protection of victims**

Globalisation and technological developments facilitate trafficking in human beings and child sexual exploitation. A variety of preventive measures, as well as measures to ensure adequate victim protection and assistance are needed, that build upon advances in social sciences and humanities.

Proposals in this subtopic should address both phenomena in a balanced way. They should ensure that the research focuses on prevention, investigation and/or assistance related to all victims of trafficking and not only addressing child trafficking. In the same way, the proposals should cover any area concerning prevention, investigation and/or assistance to victims of child sexual exploitation, not only the assistance to victims of child sexual exploitation resulting from trafficking.

With respect to the trafficking of human beings, research should bear on:

- preventing the phenomenon and to reduce the demand for all forms of exploitation in the trafficking chain and its legal and illegal sectors. The analysis of possible involvement of organized crime groups implicated in trafficking of human beings in other crimes as well (e.g., financial crimes) is recommended;
- new approaches to investigate cases involving the trafficking of human beings;
- new approaches to mitigate the impact on victims in the short and long term.

Regarding child sexual exploitation:

- how to address new threats, such as live-streaming of child abuse and coercion and extortion of victims that have escalated in the last years;
- how to provide law enforcement with effective means to detect, investigate and bring down the many peer-to-peer networks and the growing number of forums on the darknet that facilitate the exchange of child sexual exploitation material and support offenders;
- how to help victims of abuse during criminal investigations and court procedures;
- how to help the victims in the long term, to help them deal with the effects;
- how to reduce risks of (re-)offending by better understanding the behaviour of abusers and potential abusers.

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

The Internet of Things, the ever increasing number of internet-facing devices may pose substantial threats to (cyber)security as the internet has become a target for cybercriminals. The key challenge in this respect is to determine what the drivers of new forms of cyber criminality are and how they might be prevented and mitigated. The dissemination of "cybercrime-as-a-service" business models is an important enabler for crime and poses significant challenges to security. The increasing variety of such services, the modalities through which they are offered and the connections with different criminal activities need to be investigated to understand their trends and thus to allow for prevention and law enforcement.

Human factors determining online behaviour as described for instance by the online disinhibition effect (individuals acting more boldly online, being less inhibited and with their judgment impaired) are drivers for cybercrime as individuals feel disconnected from the actual crime or do not even perceive it as a crime. Recent trends also indicate a growth in cyber juvenile delinquency and a rise in adolescent hacking.

These developments call for further research in domains such as psychology, criminology, anthropology, neurobiology and cyber psychology to understand better the factors contributing to it and to devise preventive and deterrence measures, including providing alternatives to harness the potential of these young talents for cybersecurity and technologies.

- **Sub-topic 3: [2020] Developing comprehensive multi-disciplinary and multi-agency approaches to prevent and counter violent radicalisation and terrorism in the EU**
- **Sub-topic: [2018-2019] Open**

Proposals analysing and recommending other ways to solve human, social, and societal issues in fighting against crime and terrorism, and supported by large numbers of practitioners, are invited to apply under this sub-topic (see eligibility and admissibility conditions.)

Proposals should lead to solutions developed in compliance with European societal values, fundamental rights and applicable legislation, including in the area of privacy, protection of personal data and free movement of persons. Societal aspects (e.g. perception of security, possible side effects of technological solutions, societal resilience, gender-related behaviours) have to be addressed in a comprehensive and thorough manner.

The Commission considers that proposals requesting a contribution from the EU of about EUR 5 million would allow this specific challenge to be addressed appropriately through multidisciplinary projects confronting different schools of thought. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected Impact: Medium term:

- improved and consolidated knowledge among EU Law Enforcement Agencies officers on the issues addressed in this topic;
- exchange of experiences among EU Law Enforcement Agencies about human, social and societal aspects of security problems and their remedies;
- policy-making toolkits for security policy-makers, to support the establishment of a European Security Model;
- toolkits for EU Law Enforcement Agencies and/or civil society organisations, validated against practitioners' needs and requirements to facilitate their daily operations.

Long term:

- European common approaches for assessing risks/threats, and identifying and deploying relevant security measures, which take into account legal and ethical rules of operation, cost-benefit considerations, as well as fundamental rights such as the rights to privacy, to protection of personal data and the free movement of persons;
- support towards the implementation of the European Security Union by strengthening the perception by citizens of the EU as an area of freedom, justice and security;
- advances through the cross-fertilisation of concepts resulting from the collision of different ways of thinking and of different approaches developed by various partners in the proposals.

Type of Action: Research and Innovation action

The conditions related to this topic are provided at the end of this call and in the General Annexes.

SU-FCT02-2018-2019-2020: Technologies to enhance the fight against crime and terrorism[24]

Specific 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. Law Enforcement Agencies (LEAs) are often lagging behind when tackling criminal activities supported by advanced technologies.

Scope: There is a growing need to focus on technology opportunities provided by new and emerging technologies. To this end, it is necessary to identify new knowledge and targeted technologies for fighting old, new and evolving forms of criminal and terrorist behaviour supported by advanced technologies. Challenges are numerous. In conventional investigations, rapid and near real-time forensics is often crucial for preventing subsequent attacks or crimes. A consequence of the increasing digitisation of society and ever increasing adoption levels is that virtually any type of crime has a digital forensics component, which is

[24] It is expected that this topic will continue in 2020.

a challenge in itself. Money-flow tracking represents yet another challenge. The issues of location and jurisdiction need to be addressed, taking into account highly probable cross-border nature of such crimes.

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

- Sub-topic 1: [2019] Trace qualification

Forensic analysis of trace material can be extremely helpful in the initial phase of investigation, if the answers are rapid (near real-time), at an acceptable cost and compliant with criminal justice. Novel robotized or automated tools for forensic analysis should be developed. There is a need for a better knowledge and interpretation of: trace composition, time when they were left, cause of their origin (crime-related or inoffensive), etc.

- Sub-topic 2: [2018] Digital forensics in the context of criminal investigations

New forensic tools, techniques and methodologies are needed, based on common practices, standards, protocols and/or interoperability requirements that allow for rapid retrieval, storage, analysis and validation of digital evidence (including the one stored in the cloud) that upholds in court, and enables investigations to identify perpetrators as well as victims, in particular in cases of child sexual abuses. They should 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 in this domain should take into account new and emerging trends (for instance, abuse of encryption for criminal or terrorist purposes), while fully respecting fundamental rights such as the right to privacy and the right to protection of personal data.

- Sub-topic 3: [2020] Money flows tracking

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

Proposals addressing other issues relevant to this challenge (for instance: technologies to improve LEAs capabilities (including augmented reality); autonomous systems to improve the fight against crime and terrorism; technologies to support better protection of public figures; tracking and monitoring technologies, including automated prevention of uploading terrorism-related content; capabilities to detect the widest possible range of threats and concealments (including complex concealed weapons)) and supported by a large number of practitioners are invited to apply under this sub-topic (see eligibility and admissibility conditions).

In all sub-topics and in order to facilitate the EU-wide take-up of new technologies, proposers are encouraged to include the design of innovative curricula for LEAs training and (joint) exercises, and of information packages for the wider public and civil society organisations.

Proposals should lead to solutions developed in compliance with European societal values, fundamental rights and applicable legislation including in the area of privacy and protection of personal data. Societal aspects (e.g. perception of security, possible side effects of

technological solutions, societal resilience) have to be addressed in a comprehensive and thorough manner.

The centre of gravity for technology development with actions funded under this topic is expected to be up to TRL 4 to 6 – see General Annex G of the Horizon 2020 Work Programme.

The Commission considers that proposals requesting a contribution from the EU of about EUR 7 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected Impact: Medium term:

- novel, user-friendly technologies, tools and/or systems, addressing traditional or emerging forms of crime and terrorism at acceptable costs;
- improved investigation capabilities, especially regarding quality and speed;
- increased efficiency and effectiveness of the information sharing among EU LEAs.

Long term:

- prevention/reduction of criminal and terrorist threats;
- harmonisation of information formats at international level, improved cross-border acceptance and exchange of court-proof evidence, standardised evidence collection and harmonised procedures in the investigation of trans-border crimes in full compliance with applicable legislation on protection of personal data.

Type of Action: Research and Innovation action

The conditions related to this topic are provided at the end of this call and in the General Annexes.

SU-FCT03-2018-2019-2020: Information and data stream management to fight against (cyber)crime and terrorism[25]

Specific Challenge: 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.

Scope: The amount of data generated and gathered in the frame of (cyber)crime investigations increases exponentially, thereby creating a considerable challenge for law enforcement. The effectiveness of law enforcement action depends on capabilities to improve the quality of data, and to convert voluminous and heterogeneous data sets (images, videos, geospatial

[25] It is expected that this topic will continue in 2020.

intelligence, communication data, traffic data, financial transactions related date, etc.) into actionable intelligence. These capabilities could be significantly enhanced by the use of domain-specific tools, i.e. Big Data analysis applications designed for the needs of crime investigators (pre-processing, processing and analysis, visualisation, etc.). Furthermore, 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.

Examples of trends in cybercrime are numerous. The Internet of Things can potentially connect practically everything, thus also potentially making everything more vulnerable. 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. Law Eenforcement Agencies would benefit from new means of preventing and countering new kinds of crime, building on the comprehensive trend analysis of emerging cybercrime activities based on past of (cyber)criminal activities, on technological developments, and on trends in the society.

Criminal and terrorist acts are usually subsequent to patterns of abnormal behaviour. 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 suspicious events or of criminals. Such systems should operate in near real-time and at similar distances as a surveillance camera. They should also comply with privacy requirements and the respect of fundamental rights such as the right to privacy and the right to protection of personal data.

Proposals are invited from consortia involving relevant security practitioners, civil society organisations, and the appropriate balance of IT specialists, psychologists, sociologists, linguists, etc. exploiting Big Data and predictive analytics that both (a) characterise trends in cybercrime and in cybercriminal organizations (based on a profound analysis of current and emerging cybercriminal organizational types and structures), and (b) enhance citizens' security against terrorist attacks in places considered as soft targets, including crowded areas (stations, shopping malls, entertainment venues, etc.).

Proposals should lead to solutions developed in compliance with European societal values, fundamental rights and applicable legislation including in the area of privacy and protection of personal data. Societal aspects (e.g. perception of security, possible side effects of technological solutions, societal resilience) have to be addressed in a comprehensive and thorough manner.

The centre of gravity for technology development with actions funded under this topic is expected to be up to TRL 5 to 7 – see General Annex G of the Horizon 2020 Work Programme.

The Commission considers that proposals requesting a contribution from the EU of about EUR 8 million would allow this specific challenge to be addressed appropriately.

Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected Impact: Medium term:

- improved support for the work of Law Eenforcement Agencies in managing Big Data, i.e. in extracting, combining, analysing and visualising large amounts of structured and unstructured data in the context of criminal investigations;
- increased awareness regarding the state of the art and trends in cybercriminal activities (short-, mid- and long-term);
- in-depth knowledge of means of preventing and countering emerging and future cybercriminal activities;
- improved capabilities to combine and analyse in near-real-time large volumes of heterogeneous data to anticipate criminal events;
- shorter delays between the emergence of new cybercrime activities and the deployment of countermeasures.

Long term:

- a European, common strategic approach for preventing and countering an emerging cybercrime activity in its early stage of development;
- a European, common strategic approach for processing and combining huge amounts of data in the context of crowd protection in full compliance with applicable legislation on protection of personal data.

Type of Action: Innovation action

The conditions related to this topic are provided at the end of this call and in the General Annexes.

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

Type of Action:

The conditions related to this topic are provided at the end of this call and in the General Annexes.

Border and External Security

This section concerns strengthening security through border management. This includes both control and surveillance issues, on land and in the maritime domain. It contributes to the further development of the European Border Surveillance System (EUROSUR), its interoperability with other systems, and to enhance the use of new technology for border

checks, also in relation to the Smart Borders legislative initiative. It also addresses supply chain security in the context of the EU's customs policy, and migrant smuggling.

The aim of this section 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, whilst respecting fundamental rights including free movement of persons, protection of personal data, and privacy. New technologies, capabilities and solutions are also required to support the Union's external security policies in civilian tasks, ranging from civil protection to humanitarian relief, border management, law enforcement, or peace-keeping and post-crisis stabilisation, including conflict prevention, peace-building and mediation. This will also require research on conflict resolution and restoration of peace and justice, early identification of factors leading to conflict and on the impact of restorative justice processes.

Proposals are invited against the following topic(s):

SU-BES01-2018-2019-2020: Human factors, and social, societal, and organisational aspects of border and external security[26]

Specific Challenge: Border and external security may depend on a variety of human factors, and social and societal issues including gender. The adoption of appropriate organisational measures and the 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. For the purpose of this topic, 'migration' does not refer to persons enjoying the right of free movement under Article 21 TFUE and secondary legislation (i.e. Union citizens and their family members, independently of their nationality).

Scope: Proposals (which should take into account already existing tools) are invited to address related research and innovation issues, each under only one of the following sub-topics:

- Sub-topic 1: [2018] Detecting security threats possibly resulting from certain perceptions abroad, that deviate from the reality of the EU

Research should 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 possibly lead to threats and security issues on its citizens and territories, and how such perceptions can be avoided or even actively and effectively counteracted through various measures. In line with the objectives of the Union's strategy for international cooperation in research and innovation (COM(2012)497), international cooperation according to the current rules of participation is encouraged.

- Sub-topic 2: [2019] Modelling, predicting, and dealing with migration flows to avoid tensions and violence

[26] It is expected that this topic will continue in 2020.

Better modelling and predicting migration flows, based on a sound analysis and taking into account gender aspects, is required for high-level strategic decision-making, to plan and implement operational activities. For the management of the migratory flow, including relocations within the EU, it is necessary to map public sentiment, including perceptions of migration, by analysing data available from many different governmental or public sources, and by developing socio-economic indicators of integration strategies. Proposals should be solution-oriented and propose convincingly how to better deal with such flows and to reduce risks of tensions and violence among migrants and European citizens.

- Sub-topic 3: [2020] Developing indicators of threats at the EU external borders on the basis of sound risk and vulnerability assessment methodologies

- Sub-topic: [2018-2019] Open

Proposals addressing other issues relevant to this challenge, based on a sound rationale, and supported by a large number of relevant practitioners are invited to apply under this sub-topic (see eligibility and admissibility conditions.)

Proposals should lead to solutions developed, tested and validated in compliance with European societal values, fundamental rights (including gender equality) and applicable legislation including in the area of free movement of persons, privacy and protection of personal data. Societal aspects (e.g. perception of security, possible side effects of technological solutions, societal resilience) have to be analysed in a comprehensive and thorough manner with a view to facilitating future acceptance of such solutions.

Proposals should pursue truly innovative approaches. They should be submitted by consortia also involving civil society organisations. Synergies are encouraged with the work for the knowledge centre on migration and demography set up by the Commission https://ec.europa.eu/jrc/en/migration-and-demography.

The Commission considers that proposals requesting a contribution from the EU of about EUR 5 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected Impact:

- Knowledge and evidence-based support to policy developments, with fitness for purpose validated by policy-makers and by practitioners and in cooperation with civil-society organisations in the Member States, the Associated Countries, and abroad where appropriate.

- Methods to better manage the complexity (from reducing the incentives for irregular migration, to the analysis and sharing of best practices, and towards an effective application of common rules…) of the issues, with fitness for purpose validated by practitioners and civil-society organisations.

- Advances through the cross-fertilisation of concepts resulting from the collision of different ways of thinking and of different approaches developed by various partners in the proposals.

Type of Action: Research and Innovation action

The conditions related to this topic are provided at the end of this call and in the General Annexes.

SU-BES02-2018-2019-2020: Technologies to enhance border and external security[27]

Specific Challenge: Innovation for border and external security may draw, in particular, from novel technologies, provided that they are affordable, accepted by citizens and customized and implemented for the needs of security practitioners.

Scope: 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

Currently, information is made available to border and coast guards in several formats and on different kinds of hardly interoperable displays. However, human cognitive is limited at managing information from several sources simultaneously and at handling too many separate pieces of equipment is a limit to their ability to act. Furthermore, border and coast guards often work in sparsely populated and remote areas where the availability of telecommunication networks may be an issue. Research and innovation should lead towards (cloud-based) integrated systems with simple but complete and highly-standardized interfaces showing real-time information in a user-friendly way that can assist border guards in decision-making, and in remaining in contact with their command and control centre in the actual context of operations. Water, land and air operating resources should be taken into account, to lead to enhanced concept of employment, integration and interoperability standards.

- Sub-topic 2: [2018] Detecting fraud, verifying document validity, and alternative technologies to identifying people

The use of counterfeit travel documents at borders is a reality, which entails the risk of not identifying known criminals, including terrorists. It is a cross-cutting priority according to the EU Serious and Organised Crime Threat Assessment 2017[28], since it enables or enhances all types of serious and organized crime and terrorism. New countermeasures are needed to address potential frauds, in particular for the detection of morphed face images. The use of biometrics "on the fly" techniques for identification in a non-intrusive manner and without interrupting the flow of people is an area for further development, testing and validation.

- Sub-topic 3: [2019] Security on-board passenger ships

[27] It is expected that this topic will continue in 2020.

[28] https://www.europol.europa.eu/socta/2017/

Security on-board passenger ships is challenging, given the larger number of specific constraints that apply. To ensure security all along the "life cycle" of a voyage, new technologies can be implemented (together with methods for their deployment and possibly their integration into ship systems), as well as security novel procedures (including for embarkation and disembarkation, mooring at pier, etc.)

- Sub-topic 4: [2019] Detecting threats in the stream of commerce without disrupting business

The flow of goods crossing borders is increasing, whilst ways of concealing methods for dangerous materials and illegally trafficked goods are improving. The detection of such dangerous and illegal goods should be facilitated by novel technologies and sensing strategies characterized by risk-based protection and non-intrusive security checks that can be implemented without disrupting business.

Proposals should target the automation and integration of existing technologies for the purpose of identifying the largest possible amount of threat materials and ensuring the full supervision of the logistic flow of goods. This would require exploiting 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. The fitness for purpose of novel solutions should be validated at the EU external border, in a context chosen on the basis of a sound and factual risk analysis.

Of particular relevance: the enhancement of detection capabilities of contraband (mainly cigarettes) hidden in high density cargo (coal, iron ore) in particular for rail cargo transport, and well as the fight against illicit trafficking of radioactive and nuclear (NR) materials (including through the establishment of trans-European network of detection facilities with its specific concept of operations.

- Sub-topic 5: [2020] Disruptive sensor technologies for border surveillance
- Sub-topic: [2018-2019-2020] Open

Proposals addressing other issues relevant to this challenge, based on a sound rationale and supported by a large number of relevant practitioners are invited to apply under this sub-topic (see eligibility and admissibility conditions.)

Proposals should lead to solutions developed, tested, and validated in compliance with European societal values, fundamental rights and applicable legislation, including in the area of free movement of persons, privacy and protection of personal data. Societal aspects (e.g. perception of security, possible side effects of technological solutions, societal resilience) have to be addressed in a comprehensive and thorough manner.

The centre of gravity for technology development with actions funded under this topic is expected to be up to TRL 5 to 6 – see General Annex G of the Horizon 2020 Work Programme.

The Commission considers that proposals requesting a contribution from the EU of about EUR 7 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected Impact: Short term:

- Clear, realistic benchmarks against which to assess progress, so as to possibly stop the project if at mid-term review progress is not deemed sufficient.
- Plan to provide confidence in the take up of project results after the completion of the project.

Medium term:

- Evidence based knowledge, and developments performing beyond the current state of the art and leading quickly to innovation.
- Technical and operational guidelines, recommendations and best practices set in the EUROSUR handbook and in the future handbook for coast guards (as per Article 53 of the European Border and Coast Guard regulation.)

Long term:

- Implementation of solutions resulting from the legislative initiative in the "Smart Borders" package;
- Implementation of actions of civilian nature identified in the EU Maritime Security Strategy action plan;
- Implementation of the actions identified by the EU Strategy and Action Plan for customs risk management.

Type of Action: Research and Innovation action

The conditions related to this topic are provided at the end of this call and in the General Annexes.

SU-BES03-EBCGA-2018-2019-2020: Demonstration of applied solutions to enhance border and external security[29]

Specific Challenge: Solutions at high Technological Readiness Levels (TRL; please see General Annex G) to enhance border and external security do exist, but if they are not to remain unused they need to be demonstrated in the context of actual operations or exercises for validation by practitioners.

[29] This activity directly aimed at supporting pilot activities is excluded from the delegation to the Research Executive Agency and will be implemented by the European Border and Coast Guard Agency. It is expected that this topic will continue in 2020.

Part of Horizon 2020 activities related to border and external security for the period of 2018-2020 will be implemented by the European Border and Coast Guard Agency (EBCGA) in indirect management. The EBCGA will manage the phases of the project life cyle in accordance with the procedures set out in the Horizon 2020 Rules for Participation, and with due regard of Article 37 of the EBCG Regulation. To this end a delegation agreement covering the 2018-2020 activities will be concluded between the Commission and the EBCGA, setting out in details the entrusted tasks and the arrangements ensuring the protection of the financial interests of the Union.

Scope: Consortia are invited to propose demonstration of high (6-8) Technology Readiness Levels (TRL) systems applied in the context of border and external security. (TRL: please see General Annex G.)

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

- Sub-topic 1: [2018] Remotely piloted aircrafts and underwater autonomous platforms to be used from on-board offshore patrol vessels

Remotely piloted autonomous platforms of all kinds should demonstrate innovative capacities for land border and coast surveillance. Underwater autonomous platforms are also of interest for choke points surveillance (i.e. a port entrance.)

Research on artificial intelligence is likely to facilitate the transition from innovation to operation. Such platforms play an important role in facilitating long range and persistent surveillance in wide maritime areas, complementing operation from offshore patrol vessels. Improving the cost effectiveness, reliability and availability of such platforms, either by increasing the performance of existing technologies or by developing innovative concepts of operation, would notably contribute to better situational awareness at the tactical level beyond coastal waters (up to 200 nautical miles), while reducing risks during search and rescue missions, including launch and recovery phases, even in adverse sea and weather conditions. Proposals should aim at improved cost effectiveness, in particular through the remote operation of sensors mounted on aerial platforms (including optionally and remotely piloted) and by improving the on-board processing of payload data, while minimizing the data transmission to the ground segment.

- Sub-topic 2: [2019] New concepts for decision support and information systems

Information systems to support border and external security may combine a broad variety of data from very different sources, including personal data. Innovative solutions are needed to ensure the interoperability of surveillance systems, and the availability of information for maritime border surveillance coming from the area of operations in standardized formats, when and where it is needed, thus at enhancing situation awareness at strategic level (in National Coordination Centres), but also at tactical level (with assets deployed under the frame of surveillance operations). This would allow faster reaction to incidents in the maritime domain, and a reduction in the death toll at sea. Proposals should aim at optimize the exploitation of data for their specific use in surveillance is currently embryonic, and needs to

take better account of the specific characteristics of the domain, with a view to provide the needed information reducing redundancies.

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

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

Proposals addressing other issues relevant to this challenge, based on a sound rationale and with the active involvement of a large number of relevant practitioners are invited to apply under this sub-topic (see eligibility and admissibility conditions.)

Proposals submitted under this topic should be coordinated by a competent authority under civilian authority and command, nationally identified as specialised border or coast guard, or border police force.

They should clearly demonstrate how they complement and do not overlap with actions undertaken in the Preparatory Action on Defence Research under topic *PADR-US-01-2017: Technological demonstrator for enhanced situational awareness in a naval environment.*

Certain operational costs are excluded from eligible costs (see eligibility and admissibility conditions.)

Proposals should lead to solutions developed in compliance with European societal values, fundamental rights and applicable legislation, including in the area of privacy and personal data protection.

Proposals should lead to solutions developed in compliance with European societal values, fundamental rights and applicable legislation, including in the area of free movement of persons, privacy and protection of personal data.

The Commission considers that proposals requesting a contribution from the EU of about EUR 5 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected Impact: Medium term:

- Innovative solutions validated and qualified in the real, operational environment of civilian missions, defined in detail according to specifications set by the practitioners (authorities in charge of border surveillance and coast guard functions) and tailored to effectively meet their requirements within civilian missions.

- Plans for the quick take up of qualified systems at EU level.

- Plans for transnational procurement strategies.

Long term:

- Improved cost-effectiveness and efficiency of systems for the prevention of cross border crime and for border surveillance for civilian purposes.
- European standards for interoperable systems.
- Substantial and tangible improvement of (maritime) situational awareness and reaction capability, as appropriate in surveillance for civilian purposes, fight against crime, and search and rescue missions by the National and European Border and Coast Guards.
- Contribution to the concept of Common Application of Surveillance Tools, as for the European Border Surveillance System (EUROSUR) and to its interoperability with other systems.

Type of Action: Innovation action

The conditions related to this topic are provided at the end of this call and in the General Annexes.

General Matters

Proposals are invited against the following topic(s):

SU-GM01-2018-2019-2020: Pan-European networks of practitioners and other actors in the field of security[30]

Specific Challenge: In Europe, practitioners interested in the uptake of security research and innovation are dedicated to performing their duty and are focused on their tasks. In general, however, 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. All stakeholders – public services, industry, academia – including those who participate in the Security Advisory Group, recognize this as an issue.

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

a. [2019-2020] Practitioners (end-users) **in the same discipline and from across Europe** are invited to get together: 1) to monitor research and innovation projects with a view to recommending the uptake or the industrialisation of results, 2) to express common requirements as regards innovations that could fill capability and other gaps and improve their future performance, and 3) to indicate priorities as regards areas requiring more standardisation. Opinions expressed and reported by the networks of practitioners should be checked against what can be reasonably expected, and according to which timetable, from

[30] This activity directly aimed at supporting the development and implementation of evidence base for R&I policies and supporting various groups of stakeholders is excluded from the delegation to the Research Executive Agency and will be implemented by the Commission services. It is expected that this topic will continue in 2020.

providers of innovative solutions. In 2019, proposals are invited in two specific areas of specialisation: the protection of public figures; the handling of hybrid threats[31].

b. **[2018] Innovation clusters from around Europe** (established at national, regional or local level), especially those managing **demonstration sites, testing workbenches, and training facilities** (including those providing simulators, serious gaming platforms, testing of PPDR applications on broadband networks) are invited to establish one network 1) to establish and maintain a roster of capabilities and facilities, 2) to 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, and 4) to 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: 1) to share investment plans, 2) to compare procurement techniques and rules, and 3) to plan for common procurements of research services as well as of innovative, off-the-shelf products**.**

d. [2019] Border and coast guard organisations, procurement authorities, industry and researchers are invited to join forces and draft the roadmaps necessary to provide innovative, future solutions for border and coast surveillance, control and management, in the context of integrated border management and "dematerialised" borders. Whilst practitioners need to be in the lead for expressing requirements, the largest number of (national) research organisations and industry participants should also be involved in the consortium. The management of EU borders requires more interoperability among systems in order to improve capabilities. Industry is not encouraged to invest in innovation given the small size of national markets and national authorities hesitate to invest in innovative solutions not knowing the intentions of their neighbours and of other countries. A roadmap is required for border and coast guard authorities, and industry, to plan ahead and to facilitate future investments into common, interoperable solutions and systems. The roadmap should cover foresight activities, and take account of current and future relevant budget trends in the Member States and the EU.

The Commission considers that proposals requesting a contribution from the EU of:

- about EUR 3.5 million per action for a duration of 5 years (recommended duration) for Parts a), b) and d);
- about EUR 1.5 million per action for a duration of 5 years (recommended duration) for Part c)

[31] The proposal should reflect the joint communication *Joint Framework on countering hybrid threats – a European Union response* (JOIN(2016) 18 final, 6 April 2016), while keeping in mind the *Guidance note — Research with an exclusive focus on civil applications*: http://ec.europa.eu/research/participants/data/ref/h2020/other/hi/guide_research-civil-apps_en.pdf

would allow for this topic to be addressed appropriately. Nonetheless this does not preclude submission and selection of proposals requesting other amounts.

Expected Impact: Medium term:

- Common understanding of innovation potential, more widely accepted understanding, expression of common innovation and standardization needs among practitioners in the same discipline.
- Greater involvement from public procurement bodies upstream in the innovation cycle.
- More efficient use of investments made across Europe in demonstration, testing, and training facilities.

Long term:

- Synergies with already established European, national and sub-national networks of practitioners, even if these networks are for the time being only dedicated to aspects of practitioners' work unrelated to research and innovation (in general, to the coordination of their operations).

Type of Action: Coordination and support action

The conditions related to this topic are provided at the end of this call and in the General Annexes.

SU-GM02-2018-2020: Strategic pre-commercial procurements of innovative, advanced systems to support security[32]

Specific Challenge: Innovative solutions are needed when resources from different countries are required to work more closely together. Such solutions should support the development of the EU's Security Union.

Scope:

- **Sub-topic 1: [2018] Common requirements specifications for innovative, advanced systems to support security**[33]

Practitioners from several countries are invited to work on common requirements of any kind of system that they may need in the future to enhance border and external security, to fight against crime and terrorism, to protect infrastructure, or to make societies more resilient, and to involve their respective procurement bodies in preparing for future acquisitions. Practitioner organisations may be private or public entities.

[32] It is expected that this topic will continue in 2020.

[33] This activity directly aimed at supporting the development and implementation of evidence base for R&I policies and supporting various groups of stakeholders, and public-public partnerships with Member States and associated countries, is excluded from the delegation to the Research Executive Agency and will be implemented by the Commission services.

To ensure that the outcome of this action becomes also available to EU Member State national authorities as well as EU agencies not participating for further procurement purposes, 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 fully or partly derived from this action, the use of the information required to run such a procurement process, and solely for that purpose.

(2). Commitment from participating procurement authorities to consult with any legal entity generating information to be released for the purpose set out in paragraph (1), unless contrary to applicable legislation.

(3). Commitment from participating procurement authorities to negotiate the use granted under paragraph (1) on Fair Reasonable and Non-Discriminatory (FRAND) terms.

The following options of the Model Grant Agreement will be implemented:
- Options on additional exploitation obligations of Article 28.1 of the Model Grant Agreement will be applied.
- *Grants awarded under* this topic *will be complementary to the grant agreement under Sub-topic 2 of this Topic. The respective options of Article 2, and Article 41.4 of the Model Grant Agreement*[34] *will be applied.*

A subset of the domains addressed by the proposals selected for funding by the Commission further to this Call will be continued with pre-commercial procurement activities in 2020.

Proposals should lead to solutions are to be developed in compliance with European societal values,fundamental rights and applicable legislation, including in the area of free movement of persons, privacy and protection of personal data. Societal aspects (e.g. perception of security, possible side effects of technological solutions, societal resilience) have to be taken into account in a comprehensive and thorough manner. All participating procurement authorities should also commit to comply with EU data protection legislation in the development of innovative, advanced systems to support security and in particular the principles of data protection by design and by default.

The Commission considers that proposals requesting a contribution from the EU of about EUR 1 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

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

The Commission considers that proposals for pre-commercial procurement activities building upon successful activities resulting from Sub-topic 1 may require a contribution from the EU

[34] *http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/amga/h2020-amga_en.pdf*

ranging from EUR 4 to 12 million. The Commission is envisaging to dedicate about EUR 32 million to Sub-topic 2 in 2020.

Expected Impact: Short term:

- Common requirements for innovative prototypes agreed among the practitioner organisations involved in the action.
- Technical tender documents ready for use by subsequent pre-commercial procurement actions, as well as by non-participating procurement authorities.

Type of Action: Coordination and support action

The conditions related to this topic are provided at the end of this call and in the General Annexes.

SU-GM03-2018-2019-2020: Pre-commercial procurements of innovative solutions to enhance security[35]

Specific Challenge: Innovative solutions are needed when resources from different countries are required to work more closely together. Such solutions should support the development of the EU's Security Union.

Scope: Practitioners from several countries are invited to proceed with the procurement of innovative solutions to enhance their operational capability. Practitioner organisations may be private or public entities.

Phase 0: To draft common requirements for innovative prototypes, agreed among the practitioner organisations involved in the action, and to prepare the technical tender documents ready for use in the subsequent phase of the action;

Phase 1: To prepare a full tenders package for calls for tenders to build security-relevant prototypes based on the technical input resulting from Phase 0; to prepare for the validation of the future 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.

The centre of gravity for technology development with actions funded under this topic is expected to be up to TRL 8 – see General Annex G of the Horizon 2020 Work Programme.

Solutions are to be developed in compliance with European societal values, fundamental rights and applicable legislation, including in the area of free movement of persons, privacy

[35] It is expected that this topic will continue in 2020.

and protection of personal data. Societal aspects (e.g. perception of security, possible side effects of technological solutions, societal resilience) have to be addressed in a comprehensive and thorough manner. All participating procurement authorities should also commit to comply with EU data protection legislation in the development of innovative, advanced systems to support security and in particular the principles of data protection by design and by default.

The Commission considers that proposals requesting a contribution from the EU of between EUR 2 to 12 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected Impact: Short term:

- Pre-commercial prototypes matching requirements common to many Member States, and available from 2 different sources for further industrialisation.
- High leveraging effect of the EU contribution to the action.

Type of Action: COFUND (PCP)

The conditions related to this topic are provided at the end of this call and in the General Annexes.

Conditions for the Call - Security

Opening date(s), deadline(s), indicative budget(s):[36]

Topics (Type of Action)	Budgets (EUR million)			Deadlines
	2018	2019	2020	
Opening: 15 Mar 2018				
SU-BES01-2018-2019-2020 (RIA)	10.00			23 Aug 2018
SU-BES02-2018-2019-2020 (RIA)	21.00			
SU-BES03-EBCGA-2018-2019-2020 (IA)	10.00			

[36] The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The deadline(s) in 2019 and 2020 are indicative and subject to separate financing decisions for 2019 and 2020.
The budget amounts for the 2018 budget are subject to the availability of the appropriations provided for in the draft budget for 2018 after the adoption of the budget 2018 by the budgetary authority or, if the budget is not adopted, as provided for in the system of provisional twelfths.
The budget amounts for the 2019 and 2020 budget are indicative and will be subject to separate financing decisions to cover the amounts to be allocated for 2019 and for 2020.

SU-DRS01-2018-2019-2020 (RIA)	5.00			
SU-DRS02-2018-2019-2020 (RIA)	28.00			
SU-DRS03-2018-2019-2020 (IA)	6.00			
SU-FCT01-2018-2019-2020 (RIA)	10.00			
SU-FCT02-2018-2019-2020 (RIA)	21.00			
SU-FCT03-2018-2019-2020 (IA)	8.00			
SU-GM01-2018-2019-2020 (CSA)	5.00			
SU-GM02-2018-2020 (CSA)	6.00			
SU-GM03-2018-2019-2020 (COFUND-PCP)	8.20			
Opening: 14 Mar 2019				
SU-BES01-2018-2019-2020 (RIA)		9.60		22 Aug 2019
SU-BES02-2018-2019-2020 (RIA)		21.00		
SU-BES03-EBCGA-2018-2019-2020 (IA)		10.00		
SU-DRS01-2018-2019-2020 (RIA)		5.00		
SU-DRS02-2018-2019-2020 (RIA)		21.00		
SU-DRS03-2018-2019-2020 (IA)		6.00		
SU-DRS04-2019-2020 (RIA)		10.50		
SU-DRS05-2019 (IA)		10.00		
SU-FCT01-2018-2019-2020 (RIA)		9.60		
SU-FCT02-2018-2019-2020 (RIA)		28.16		
SU-FCT03-2018-2019-2020 (IA)		8.00		
SU-GM01-2018-2019-2020 (CSA)		10.50		
SU-GM03-2018-2019-2020 (COFUND-PCP)		7.00		
Opening: To be defined				
Focus area topic(s) for 2020			185.00	To be defined

Overall indicative budget	138.20	156.36	185.00	

Indicative timetable for evaluation and grant agreement signature:

For single stage procedure:

- Information on the outcome of the evaluation: Maximum 5 months from the final date for submission; and
- Indicative date for the signing of grant agreements: Maximum 8 months from the final date for submission.

Eligibility and admissibility conditions: The conditions are described in General Annexes B and C of the work programme. The following exceptions apply:

SU-DRS01-2018-2019-2020	This topic requires the active involvement of at least 3 first responders' organisations or agencies from at least 3 different EU or Associated countries.
SU-DRS02-2018-2019-2020, SU-DRS03-2018-2019-2020	Predefined sub-topics require the active involvement of at least 3 agencies or first responders' organisations from at least 3 different EU or Associated countries. Where applicable, Sub-topic: Open requires the active involvement of at least 5 such organisations, from at least 5 different EU or Associated countries.
SU-DRS04-2019-2020	Each RIA must establish its standard consortium agreement, as well as a "Collaboration Agreement" with participant(s) in the ENCIRCLE consortium. A draft of the "Collaboration Agreement" must be attached to the RIA proposal, and endorsed by at least one participant in ENCIRCLE. All beneficiaries of the RIA grant agreements must be independent from each beneficiary in the ENCIRCLE consortium. Each RIA proposal must be coordinated by an SME.
SU-DRS05-2019	This topic requires the active involvement of organizations in charge of national planning in relations with pandemics preparedness, from at least 5 different EU or Associated countries. This topic requires the active involvement of at least 3 first responder organizations, from at least 3 different EU or Associated countries.

	The duration of the proposed activity must not exceed 24 months.
SU-FCT01-2018-2019-2020, SU-FCT02-2018-2019-2020	Predefined sub-topics require the active involvement of at least 3 Law Enforcement Agencies (LEAs) from at least 3 different EU or Associated countries. Where applicable Sub-topic: Open requires the active involvement of at least 5 such organisations, from at least 5 different EU or Associated countries.
SU-FCT03-2018-2019-2020	This topic requires the active involvement of at least 3 Law Enforcement Agencies (LEAs) from at least 3 different EU or Associated countries. The duration of the proposed activities must not exceed 24 months.
SU-FCT04-2020	Participation is required of at least 6 relevant practitioner organisations from at least 3 different EU or Associated countries.
SU-BES01-2018-2019-2020, SU-BES02-2018-2019-2020, SU-BES03-EBCGA-2018-2019-2020	Predefined sub-topics require the active involvement of at least 3 Border or Coast Guards Authorities from at least 3 different EU or Associated countries. Where applicable Sub-topic: Open requires the active involvement of at least 5 such organisations, from at least 5 different EU or Associated countries.
SU-BES03-EBCGA-2018-2019-2020	Consortia must be coordinated by a practitioner organization under civilian authority and command. The duration of the proposed activities must not exceed 18 months.
SU-GM01-2018-2019-2020	**For part a):** Practitioner participation from at least 8 Member States or Associated Countries is mandatory. 1. Each proposal must include a plan, and a budget amounting at least 25% of the total cost of the action, to interact with industry, academia, and other providers of innovative solutions outside of the consortium, with a view to assessing the feasibility of their findings; 2. Each consortium must commit to produce, every 6 or fewer months, a report about their findings in the 3 lines of

	actions (see in "Scope"); 3. Each proposal must include a workpackage to disseminate their findings, including an annual workshop or conference 4. **part a)** is opened only in 2019. The Commission may, at the opening of the Call in 2019, provide more details about the professional areas eligible at the time, better to take account of the areas covered in previous Calls. **For part b), and c):** Practitioner participation from at least 8 Member States or Associated Countries is mandatory. 1. Each consortium must commit to produce, every 6 or fewer months, a report about their findings in the 3 lines of actions (see in "Scope"); 2. Each proposal must include a workpackage to disseminate their findings, including an annual workshop or conference; 3. Only one network under each of part b), c) and d) may be supported over the 2018-2019 period. **For part d):** Practitioner participation from at least 8 Member States or Associated Countries is mandatory. 1. Each consortium must commit to produce and update, every 12 or fewer months, a roadmap for both border and coast guards, and industry to plan ahead so as to facilitate investments into common, interoperable solutions for border security. 2. Each proposal must include a workpackage to disseminate their findings, including an annual workshop or conference; 3. Only one such network may be supported over the 2018-2019 period.
SU-GM02-2018-2020	In the Sub-topic called for in 2018 (Sub-topic 1), Participation is

	required of at least 6 relevant practitioner organisations, as well as of 3 potential "buyers" of systems (e.g. departments or agencies dealing with acquisition planning, or procurement), from 3 different EU or Associated countries. In the Sub-topic called for in 2020 (Sub-topic 2), Participation is required of at least 3 relevant practitioner organisations, as well as of 3 potential "buyers" of systems (e.g. departments or agencies dealing with acquisition planning, or procurement), from 3 different EU or Associated countries.
SU-GM03-2018-2019-2020	Participation is required of at least 3 relevant practitioner organisations, as well as of 3 potential "buyers" of systems (e.g. departments or agencies dealing with acquisition planning, or procurement), from 3 different EU or Associated countries.

Evaluation criteria, scoring and threshold: The criteria, scoring and threshold are described in General Annex H of the work programme.

Evaluation Procedure: The procedure for setting a priority order for proposals with the same score is given in General Annex H of the work programme. The following exceptions apply:

SU-BES01-2018-2019-2020, SU-BES02-2018-2019-2020, SU-BES03-EBCGA-2018-2019-2020, SU-DRS02-2018-2019-2020, SU-FCT01-2018-2019-2020, SU-FCT02-2018-2019-2020, SU-GM01-2018-2019-2020	Grants will be awarded to proposals according to the ranking list. However, in order to ensure a balanced portfolio of supported actions, at least the highest-ranked proposal per sub-topic will be funded provided that it attains all thresholds.

The full evaluation procedure is described in the relevant guide published on the Participant Portal.

Grant Conditions:

SU-BES03-EBCGA-2018-2019-2020	For grants awarded under this topic, the following cost categories will be ineligible costs: Cost of fuel The respective option of Article 6.5(c) [MSCA: 6.3] of the

	Model Grant Agreement will be applied.
SU-GM03-2018-2019-2020	As an exception from General Annex H for grants awarded under the Sub-topic called for in 2020 (Sub-topic 2) under this topic, funding rate for direct costs is maximum 70% of the eligible costs. Given the broad openess of the topic, the amount invested by the buyers contributes to demonstrate their commitment and the interest in the outcome of the action. The applicants may request a funding rate lower than 70%, so as to increase the leveraging effect of the EU contribution to the action.
SU-GM02-2018-2020, SU-GM03-2018-2019-2020	For grants awarded under this topic the beneficiaries must grant access rights for EU institutions, bodies, offices or agencies and Member States under the special conditions for for the Specific Objective 'Secure societies - Protecting freedom and security of Europe and its citizens'. The respective option of Article 31.5 of the Model Grant Agreement will be applied.

Consortium agreement:

SU-BES01-2018-2019-2020, SU-BES02-2018-2019-2020, SU-BES03-EBCGA-2018-2019-2020, SU-DRS01-2018-2019-2020, SU-DRS02-2018-2019-2020, SU-DRS03-2018-2019-2020, SU-DRS04-2019-2020, SU-DRS05-2019, SU-FCT01-2018-2019-2020, SU-FCT02-2018-2019-2020, SU-FCT03-2018-2019-2020, SU-FCT04-2020, SU-GM01-2018-2019-2020, SU-GM02-2018-2020, SU-GM03-2018-2019-2020	Members of consortium are required to conclude a consortium agreement, in principle prior to the signature of the grant agreement.

Call - Digital Security[37]

H2020-SU-DS-2018-2019-2020

This Call deals with R&D and innovation towards enhancing digital security.

Proposals under this call should consider the relevant human factor and social aspects when developing innovative solutions. Where relevant, proposals should also describe how the gender dimension is taken into account in their content.

Whereas activities will have an exclusive focus on civil applications, coordination with the activities of the European Defence Agency (EDA) may be considered with possible synergies being established with projects funded by the EDA programmes[38]. The complementarity of such synergies should be described comprehensively. On-going cooperation should be taken into account. Only an explicit and firm commitment from EDA-funded projects to contribute to a project may positively impact the evaluation of a proposal submitted under this work programme part.

In this Call, "standards" and "standardisation" are used in a broad sense, except where they are specifically referred to as "European standards" or "European standardisation".

For grants awarded under these topics for Innovation Action and/or Research and Innovation Action, the Commission or Agency may object to a transfer of ownership or the exclusive licensing of results to a third party established in a third country not associated to Horizon 2020. The respective option of Article 30.3 of the Model Grant Agreement will be applied.

All topics in this work programme part will be subject to security scrutiny.

Cybersecurity, Digital Privacy and data protection

The aim of this Call is to ensure society as a whole benefits 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.

Trust and security are at the core of the Digital Single Market Strategy[39]*, while the fight against cybercrime is one of the three pillars of the European Agenda on Security*[40]*. The new set of measures in the area of cybersecurity building on previous actions has been recently announced in the Joint Communication to the European Parliament and the Council "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU"*[41].

[37] It is expected that this call will continue in 2020.

[38] http://eda.europa.eu/what-we-do/eda-priorities/research-technology

[39] *Communication "A Digital Single Market Strategy for Europe" of 6.5.2015 - COM(2015) 192 final*

[40] *Communication "The European Agenda on Security" of 28.4.2015 – COM (2015) 185 final*

[41] *JOIN(2017) 450 final, Brussels, 13.9.2017*

The compliance of the European infrastructures, products and services with relevant directives (e.g. NIS [42] *, Data Protection Directive for Police and Criminal Justice Authorities*[43]*), regulations (e.g. eIDAS*[44]*, GDPR*[45]*, proposal for an e-Privacy regulation*[46]*) and standards (e.g. ISO27001, ISO27005) will promote trust and confidence to the European consumers and providers/suppliers, paving the way for a competitive, trustworthy Digital Single Market. Innovative solutions and services in digital security, privacy and personal data protection will open new market opportunities for the EU companies and will ensure a secure and trusted networked environment for the governments, businesses, individuals and smart things. Cybersecurity and privacy technologies will significantly contribute to strengthen the competitiveness of the EU industry and will enable its development as world leader in the global market.*

The Communication on "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry"[47] shaped the main related challenges and several strategic initiatives to address them. Established in July 2016, the contractual Public Private Partnership (cPPP) on Cybersecurity aims at building trust among Member States and industry by fostering cooperation at early stages in the research and innovation process and helping to align demand and supply. It has been an important mean of consultation for defining research and innovation priorities for 2018-2020 and it will facilitate the engagement of end-users in sectors that are important beneficiaries and customers of cybersecurity solutions (e.g. energy, transport, health, finance) towards defining and providing to the industry their sector-specific digital security, privacy and personal data protection common requirements. The topics below belonging to this Digital Security call are part of the contribution of the Commission to the Cybersecurity cPPP.

Proposals are invited against the following topic(s):

SU-DS01-2018: Cybersecurity preparedness - cyber range, simulation and economics

Specific Challenge: The digital infrastructure, upon which other sectors, businesses and society at large critically depend, must be resilient and trustworthy, and must remain secure despite the escalating cyber-threats. New technologies and their novel combinations require

[42] *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)*

[43] *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*

[44] *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*

[45] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*

[46] *Proposal for a Regulation of the European Parliament and of the Council - COM(2017) 10 final of 10.1.2017*

[47] COM(2016) 410 final, Brussels, 5.7.2016

innovative ways to implement security measures and to make new security-related assumptions, identifying "zero-day" or potential unknown vulnerabilities, forecasting new threats (plus their cascading effects) and emerging attacks, and managing cyber risks.

Many organisations are unable to forecast and/or estimate the impacts of a cyber-risk. This results often in insufficient and/or irrelevant investments to ensure a more cyber secure environment. In addition, cybersecurity experts and professionals need to continuously adapt their expertise to a constantly evolving landscape with increasingly sophisticated and novel cyber-attacks, a widening surface of exposed ICT systems and services and a set of relevant changing legislation. In a connected EU society, there is an urgent need for highly competent cybersecurity professionals, and security experts need to be in a constant learning process, to match the quick rate of evolution of the cyber threats, attacks and vulnerabilities.

Cybersecurity skills need to be continuously advanced at all levels (e.g. security officers, operators, developers, integrators, administrators, end users) in order to enable cybersecurity, digital privacy and personal data protection within the EU Digital Single Market.

Scope: As a continuation of topic DS-07-2017 "Addressing advanced cyber security threats and threat actors", where cyber range is partially addressed, proposals are called to deliver extended capabilities of cyber ranges (e.g. piloting of networked cyber-ranges; extension of the cyber-ranges network, adding domain specificities like cyber range for IoT and/or for Industrial Control Systems such as SCADA).

The proposals should develop, test and validate highly customizable dynamic simulators serving as knowledge-based platforms accompanied with mechanisms for real time interactions and information sharing, feedback loops, developments and adjustments of exercises. These simulation platforms will help professionals responsible for cybersecurity in organizations to collaboratively improve their ability in handling and forecasting security incidents, complex attacks and propagated vulnerabilities, based upon targeted scenarios and exercises. Proposals are encouraged to bring shared approaches to express and transform user needs into actual experiments and cyber exercises (e.g. capture-the-flag) and to develop/integrate/parameterise appropriate tools and methods for supporting current and future generated evidence-based simulation scenarios. The proposed cyber range model should be validated across one critical economic sector, involving as many as possible relevant stakeholders from its supply chain. Proposals should consider the specific needs of end-users, private and public security end-users alike. Proposals are encouraged to include public security end-users and/or private end-users, and to create operational links to the Computer Emergency Response Teams (CERTs) / Computer Security Incident Response Teams (CSIRTs)[48] network across the EU.

Proposals should also develop, test and validate operational ways to continuously analyse the information collected by CERTs and/or CSIRTs and all relevant cybersecurity data. This analysis should feed their risk analysis models (which need to comply with relevant standards

[48] Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS directive)

e.g. ISO27001, ISO27005 and relevant EU cybersecurity legislation) in order to derive appropriate econometric models that can be used by public/private organisations/companies (e.g. insurance companies, SMEs, governmental bodies). These econometric models should assist them to select realistic, affordable baseline cybersecurity measures that will improve their security, resilience and sustainability, and should also help in identifying the cost and time to recover following a cyber-attack.

In addition, the proposals should show that the econometric models contribute to: (i) identifying affordable security controls that are needed to protect valuable organization assets, (ii) promoting the development of cyber insurance and liability policies/contracts and (iii) fostering service level agreements addressing security, privacy and personal data protection requirements and policies. Proposals should bring innovative solutions to enforce and encourage accountability of security as a shared responsibility.

Proposals should also include (but should not be limited to) the delivery of solutions for specific social aspects of digital security related to training, in particular practical, operational and hands-on training, including: (i) increasing the dynamics of the training and awareness methods, to match/exceed the same rate of evolution of the cyber attackers, that is to say new methods of awareness/training offering more qualification tracks to fully and efficiently integrate ICT security workers and employers in the European e-Skills market; and (ii) integrating 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.

The outcome of the proposal is expected to lead to development up to Technology Readiness level (TRL) 7; please see Annex G of the General Annexes.

The Commission considers that proposals requesting a contribution from the EU of between EUR 5 and 6 million would allow the specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Projects should also foresee activities and envisage resources for clustering with other projects funded under this topic and with other relevant projects in the field funded by H2020.

Expected Impact:

Short-term:

- Professionals better prepared to detect, block and mitigate emerging cyberattacks;
- End-users of cybersecurity products and services more involved into expressing actual needs to developers/vendors, through cyber range and simulation;
- More organized collaboration between a network of cyber ranges and Europe-wide initiatives such as the CERTs/CSIRTs cooperation network of the NIS directive.

- Improved risks analysis models to be used by public/private organisations, through the use of economics for evidence-based cybersecurity and data privacy;
- Appropriate econometric models able to learn from cyber incident data on a wide scale;
- Improved knowledge on how organisations can make the right investment to secure their operations against cyber-attacks (e.g. where they result in personal data breaches[49]), using economics for evidence-based cybersecurity and data privacy;

Medium and long term:

- Improved resilience of ICT systems/infrastructures and reduced time and cost in infrastructures for training users;
- EU member states better prepared to face malware campaigns and to take down malicious infrastructures; improved EU-skills market;
- Better preparedness to put in place cybersecurity measures and identify the necessary resources for recovering after a cyber-attack;
- Improved security, resilience and sustainability of organisations.

Type of Action: Innovation action

The conditions related to this topic are provided at the end of this call and in the General Annexes.

SU-DS02-2020: Management of cyber-attacks and other risks

Type of Action:

The conditions related to this topic are provided at the end of this call and in the General Annexes.

SU-DS03-2019-2020: Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises[50]

Specific Challenge: Some members of the digital society in the EU are more vulnerable as they are less prepared to confront with cyber-attacks. The scale, value and sensitivity of personal data in the cyberspace are significantly increasing and citizens are typically uncertain about who monitors, accesses and modifies their personal data. Personal data breach may facilitate abuse by third parties, including cyber-threats such as coercion, extortion and corruption.

[49] Notification of a personal data breach to the supervisory authority and communication of a personal data breach to the data subject are regulated under articles 33 and 34 of the GDPR.

[50] It is expected that this topic will continue in 2020.

In order to protect the freedom, security and privacy, and ensure personal data protection of the citizens in Europe, citizens should be enabled to assess the risk involved in their digital activities and configure their own security, privacy and personal data protection settings and controls across these services. Citizens need to be fully aware that their informed consent is necessary in many situations and become capable in providing their permission/consent for allowing accessing their personal data/devices/terminals with an increased level of granularity. Additionally there is a need for increased citizens' capacity to modulate the level and accuracy of the monitoring tools used by services (e.g. via cookies, positioning, tokens).

Most Small and Medium-sized Enterprises and Micro Enterprises (SMEs&MEs) lack sufficient awareness and can only allocate limited resources - both technical and human - to counter cyber risks, hence they are an easier target (e.g. of ransomware attacks) compared to large organizations. Security professionals and experts working for SMEs&MEs need to be in a constant learning process since cybersecurity is a significantly complex and fast-evolving field. Taking into account the significant economic role of SMEs&MEs in the EU, tailored research to innovation should support cybersecurity for SMEs&MEs.

Scope: Proposals are invited against one of the following sub-topics:

(a): Protecting citizens' security, privacy and personal data

Proposals should bring innovative solutions to personal data protection, develop new applications and technologies in order to help citizens to better monitor and audit their security, privacy and personal data protection, enabling them to become more engaged and active in the fight against cyber, privacy and personal data protection risks.

These solutions should include innovative approaches, techniques and user-friendly tools for: (1) improving resilience against privacy and personal data protection risks (e.g. personal data breaches[51]) and cyber threats (e.g. profiling, eavesdropping, data misuse); (2) identifying, removing and reporting potential harmful content (e.g. apology of criminal acts, unhealthy or self-harming habits) and abusive interactions (e.g. harassment, unsolicited communications); (3) exercising citizens' right to erasure ("right-to-be-forgotten")[52] and data portability[53]; (4) providing citizens with transparent information about their privacy and personal data protection[54] level and empowering them to modulate it at any moment of their digital activities (e.g. by activating encryption); (5) protecting or providing rights for any access/audit/interference with citizens' "smart terminals" or their Internet-based communications in a data protection compliant way; (6) developing on-line help-desks services or "one-stop-shop" informing, helping citizens in dealing with any security and/or privacy incident and data (including personal data) protection breach, and enabling them in reporting any cyber or privacy related incident and data (including personal data) protection breach. Such approaches need to build bridges/synergies with data protection authorities and

[51] Notification off a personal data breach to the supervisory authority and communication of a personal data breach to the data subject are regulated respectively under articles 33 and 34 of the GDPR.

[52] See article 17 of the GDPR.

[53] See article 20 of the GDPR.

[54] See article 12 of the GDPR.

CERTs/CSIRTs. To better respond to the needs and expectations of the end-users, proposals should engage the end-users by involving them in the design and implementation, in order to ensure the usability and acceptability of the proposed solutions. In addition, assurance and transparency about the digital security, privacy and personal data protection levels embedded in products and services should be easily accessed, identified and monitored by all citizens, independently of their physical condition or ICT skills, by developing appropriate innovative solutions.

The outcome of the proposal is expected to lead to development up to Technology Readiness level (TRL) 7; please see Annex G of the General Annexes.

The Commission considers that proposals requesting a contribution from the EU of between EUR 4 and 5 million would allow this specific challenge under sub-topic (a) to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

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

Proposals should deliver innovative solutions to increase the knowledge sharing in digital security across SMEs&MEs and between SMEs&MEs and larger providers. The user SMEs&MEs should be supported by democratizing access to tools and solutions of varied sophistication level, to allow SMEs&MEs benefitting from innovative targeted solutions addressing their specific needs and available resources (currently reserved to larger organisations, due to their cost and availability of internal expertise).

The proposals should develop targeted, user-friendly and cost-effective solutions enabling SMEs&MEs to: (1) dynamically monitor, forecast and assess their security, privacy and personal data protection risks[55]; (2) become more aware of vulnerabilities, attacks and risks that influence their business; (3) manage and forecast their security, privacy and personal data protection risks in an easy and affordable way; (4) build on-line collaboration between SMEs&MEs associations and with CERTs/CSIRTs, enabling thus individual SMEs&MEs to report any incident.

In addition, tools and processes should be proposed to facilitate the participation of user SMEs&MEs in cyber ranges for cybersecurity.

The outcome of the proposal is expected to lead to development up to Technology Readiness level (TRL) 7; please see Annex G of the General Annexes.

The Commission considers that proposals requesting a contribution from the EU of between EUR 3 and 4 million would allow this specific challenge under sub-topic (b) to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

[55] Data protection impact assessments are required in situation enumerated in article 35 of the GDPR.

Projects should also foresee activities and envisage resources for clustering with other projects funded under this topic and with other relevant projects in the field funded by H2020.

Expected Impact:

- Citizens and SMEs&MEs are better protected and become active players in the Digital Single Market, including implementation of the NIS directive and the application of the General Data Protection Regulation.
- Security, privacy and personal data protection are strengthened as shared responsibility along all layers in the digital economy, including citizens and SMEs&MEs.
- Reduced economic damage caused by harmful cyber-attacks and privacy incidents and data (including personal data) protection breaches.
- Pave the way for a trustworthy EU digital environment benefitting all economic and social actors.

Type of Action: Innovation action

The conditions related to this topic are provided at the end of this call and in the General Annexes.

SU-DS04-2018-2020: Cybersecurity in the Electrical Power and Energy System (EPES): an armour against cyber and privacy attacks and data breaches[56]

Specific Challenge: The Electrical Power and Energy System (EPES) is of key importance to the economy, as all other domains rely on the availability of electricity, hence a power outage can have direct impact on the availability of other services (e.g. transport, finance, communication, water supply) where backup power is not available or the power restoration time goes beyond the backup autonomy.

With the transition to a decentralised energy system, digital technologies are playing an increasingly important role in the EPES: they contribute reducing the energy consumption; they enable the integration of higher shares of renewables and promote a more energy efficient system. At the same time, with the growing use of digital devices and more advanced communications and interconnected systems, the EPES is increasingly exposed to external threats, such as worms, viruses, hackers and data privacy breaches.

Without appropriate cyber-defence measures, systems access could be violated (e.g. with the malware spreading over the system) and may cause power outages, damages and cascading effects to interconnected systems, and energy services. Therefore, with increased digitalisation, the EPES will face an increasing range of threats requiring an attentive evaluation of the cyber security risk that allows taking proper countermeasures. For example, the growing use of interconnected smart devices in the EPES will increase the number of access points (e.g. smart meters, IoT), hence increasing the exposure to cyberattacks. Also,

[56] It is expected that this topic will continue in 2020.

even if security improvements may have been made since, older technologies used in legacy systems such as SCADA/ICS (Supervisory Control and Data Acquisition System/Industrial Control Systems) were designed in times when cybersecurity was not part of the technical specifications for the system design.

On the other side, a control system in the EPES that is under attack might not be easily disconnected from the network as this could potentially result in safety issues, brownouts or even blackouts. At the same time, with the decentralisation leading to a distributed energy system, microgrid operations and/or islanding could be further exploited against cyber-attacks and cascading effects in the EPES.

In order 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 detecting and preventing threats with severe impacts and to shield the electric system against cyber-attacks. Without an adequate strategy and measures to protect the energy system from cyber-attacks, the energy transition would be more risky, more costly and possibly in danger.

Scope: The proposals should demonstrate how the actual EPES can be made resilient to growing and more sophisticated cyber and privacy attacks and data breaches (including personal data breaches) taking into account the developments of the grid towards a decentralised architecture and involving all stakeholders. The proposals should demonstrate the resilience of the EPES through the design and implementation of adequate measures able to make assets and systems less vulnerable, reducing its expositions to cyberattacks. Different scenarios of attacks with the expected potential disruptive effects on the EPES should be envisaged and the relative counteracting measures should be designed, described, tested (sandboxing, simulations) on a representative energy demonstrator to verify effectiveness. Depending on the specific application, the proposal should apply measures to new assets or to existing equipment where data flows were not designed to be cyber protected (e.g. SCADA, ICS). The proposals shall implement the following series of activities to make the electric system cyber secure: (i) assessing vulnerabilities and threats of the system in a collaborative manner (involving all stakeholders in the energy components provision supply chain); (ii) on that basis, designing adequate security measures to ensure a cyber-secure system and describing the advantages of the solutions adopted compared to others and which aim to guarantee the level of cybersecurity and resilience vital for EPES in an evolving system; (iii) implementing both organisational and technical measures in representative demonstrator to test the cyber resilience of the system with different types of attacks/severity; and (iv) demonstrating the effectiveness of the measures with a cost-benefit analysis. The activities may include the testing of micro-grid and/or islanding as a means to reduce the vulnerability to cyber-attacks.

The proposals shall also (i) 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 CERTs; (ii) define cybersecurity design principles with a set of common requirements to inherently secure

EPES; (iii) formulate recommendations for standardisation and certification in cybersecurity at component, system and process level; and (iv) propose policy recommendations on EU exchange of information.

The dimension of a pilot/demonstrator within the proposal should be at large scale level (e.g. neighbourhood, city, regional level), involving generators, one primary substation, secondary substations and end users. The proposals are encouraged to include the following types of entities: TSO, DSO, electricity generators, utilities, equipment manufacturers, aggregators, energy retailers, and technology providers.

The proposals may refer to Industry 4.0 and other proposals and/or projects dealing with cybersecurity in energy.

Projects should also foresee activities and envisage resources for clustering with other projects funded under this topic and with other relevant projects in the field funded by H2020, in particular under the BRIDGE initiative[57].

The outcome of the proposal is expected to lead to development up to Technology Readiness level (TRL) 7; please see Annex G of the General Annexes.

The Commission considers that proposals requesting a contribution from the EU of between EUR 6 and 8 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Expected Impact:

- Built/increased resilience against different levels of cyber and privacy attacks and data breaches (including personal data breaches) in the energy sector.
- Ensured continuity of the critical business energy operations.
- The energy sector is better enabled to easily implement the NIS directive.
- A set of standards and rules for certification of cybersecurity components, systems and processes in the energy sector will be made available.
- Cyber protection policy design and uptake at all levels from management to operational personnel, in the energy sector.
- Manufacturers providing more accountability and transparency, enabling third parties monitoring and auditing the privacy, data protection and security of their energy devices and systems.

Type of Action: Innovation action

[57] http://www.h2020-bridge.eu/

The conditions related to this topic are provided at the end of this call and in the General Annexes.

SU-DS05-2018-2019: Digital security, privacy, data protection and accountability in critical sectors

Specific Challenge: In critical vertical sectors/domains, cybersecurity technologies deployed in several application domains should be aligned to the specific domain needs, linking the demand and supply sides for such cyber technologies. In the context of an increased digitization and also of growing complexity of cyber-attacks, there are certain sectors/subsectors identified as critical from the point of view of cybersecurity needs in the NIS Directive: energy (electricity, oil, gas), transport (air transport, rail transport, water transport, road transport), banking, financial market infrastructures, health sector (health care settings, including hospitals and private clinics), drinking water supply and distribution, and digital infrastructure. These sectors are important customers of cybersecurity solutions; hence it is of outmost importance to facilitate the engagement of end-users towards defining and providing sector-specific common requirements about digital security, privacy and personal data protection. Building security, privacy and personal data protection by design and by default, principles and standards should be clearly defined to protect the critical infrastructures in these sectors and ensure personal data integrity and confidentiality.

For transport domain, security must be managed pro-actively over the system as a whole. This must also extend to include interfaces to critical supporting infrastructures such as communication networks and satellite systems. The complexity of the transport sector finds its roots in the diversity of components that build the solutions in use and the very long lifecycle of these components. The challenge is to migrate these solutions, systems, and infrastructures to a higher level of cybersecurity.

ICT enables the healthcare sector to provide efficient, effective, cross-border top-quality healthcare services improving the public healthcare. Healthcare operations, services and applications are provided via various interconnected infrastructures, systems, entities and people. Personalized medicine is on the brink of becoming a successful approach in treating diseases. This increases the complexity of the pharmaceutical supply chain and raises the importance of achieving a zero error rate in the supply of personalized medications. Cybersecurity in this respect is safety critical and novel approaches are needed to ensure traceability and zero error deliveries. Moreover, requirements related to data protection legislation should also be taken into account, as health is a very sensitive sector from this point of view[58].

This interconnectivity reveals various threats, making the healthcare ecosystem vulnerable to catastrophic attacks with high impact to healthcare institutions and people's lives. The healthcare industry has seen a major rise in cyber-attacks over the past two years, and data breaches increasingly damage the healthcare industry as well as the privacy and personal data

[58] The GDPR in its Article 9 (processing of special categories of personal data) prohibits the processing of personal data concerning health unless one of the conditions set out in Article 9(2) apply.

protection of the people. Vulnerable patients' records management systems can be attacked leading to unauthorised disclosure of and access to personal data concerning health. Connected medical devices are increasingly used, in particular wearables and home health monitoring devices which often transmit sensitive data over unsecure wireless networks from the patients' home to the hospitals exposing the privacy and personal data of the patients and the resilience of the healthcare infrastructures.

Digital technologies are also profoundly changing the financial sector. Cybersecurity solutions are essential to make possible digital technologies for finance and for the stability of the financial sector which must respond to increasingly sophisticated cyber-attacks.

Scope: Among the critical sectors mentioned in the NIS Directive[59], proposals should treat generic aspects for at least two of them, by identifying common threats and attacks, and by developing proof of concepts for managing cybersecurity and privacy risks. In addition, proposals should treat specific aspects for one of the three critical sectors/domains mentioned as sub-topics, i.e. transport, healthcare and finance, by identifying specific vulnerabilities, propagation effects and counter measures, by developing and testing cyber innovation-based solutions and validating them in pilots/demonstrators. During the conception and development steps, critical sectors/domains' specificities, such as complexity of infrastructure and their large scale, should be taken into account. These pilots/demonstrators are encouraged to use relevant transversal cyber infrastructures and capabilities developed in other projects.

Proposals should also include (but should not be limited to) the delivery of specific social aspects of digital security related to training, in particular practical, operational and hands-on training, including: (i) increasing the dynamics of the training and awareness methods, to match/exceed the same rate of evolution of the cyber attackers; that is to say new methods of awareness/training offering more qualification tracks to fully and efficiently integrate ICT security workers and employers in the European e-Skills market; and (ii) integrating 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.

Proposals are invited against the following sub-topics below, in 2018 and 2019

(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. A European Single Transport market requires a pan-European, seamless privacy aware solution to access across mass, shared and individual mobility, which will bring added value to citizens while safeguarding data protection and privacy. However the corresponding increased interconnection of smarter systems increases the vulnerability surface and therefore novel tailored solutions should be proposed.

[59] NIS directive - Annex II .

(2): Assurance and protection against specific cyber-attacks in the multimodal transport domain, addressing interconnected threats and propagated vulnerabilities. Feasible solutions in practice should be delivered, shielding the vulnerabilities that have severe impact and catastrophic propagation effects to the multimodal transport operations. Applicants should propose integrated, holistic approaches and tools for dynamically, automatically forecast and manage complex security and privacy incidents, and personal data breaches in the multimodal transport service and operation. Proposals should improve the security intelligence of treating complex multimodal transport security and privacy incidents, notably personal data breaches, vulnerabilities and attacks. Proposals should develop practical solutions 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. Proposals should evaluate the feasibility of a security labelling for transport and deliver relevant recommendations and options.

The outcome of the proposal is expected to lead to development up to Technology Readiness level (TRL) 7; please see Annex G of the General Annexes.

The Commission considers that proposals requesting a contribution from the EU of about EUR 5 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Type of Action: Innovation action

(b) [2019]: Digital security, privacy and personal data protection in healthcare ecosystem

Proposals responding to this sub-topic should contribute towards the practical implementation of relevant EU legislation (e.g. NIS, eIDAS and GDPR) in the healthcare complex ecosystem involving all stakeholders (e.g. security officers, ICT administrators, operators, auditors, developers, manufactures, integrators, data protection officers) of all entities in the healthcare ecosystem and considering all types of data handled, with special focus on sensitive data as defined by the GDPR.

Proposals under this sub-topic should tackle 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 (enhancing the ICT generic ones e.g. NIST, MITRE). 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, and propagated vulnerabilities in interconnected healthcare infrastructures, entities, systems, supply chain services and applications (compliant with appropriate cybersecurity standards e.g. ISO27001, ISO27005, ISO28000).

(3): Provide collaborative privacy-aware tools enabling healthcare stakeholders to access and share information (where its integrity is guaranteed), advise and provide best/good practices about incident handling through appropriate interaction with healthcare participants respecting their privacy and personal data protection.

The outcome of the proposal is expected to lead to development up to Technology Readiness level (TRL) 7; please see Annex G of the General Annexes.

The Commission considers that proposals requesting a contribution from the EU of about EUR 5 million would allow this specific challenge to be addressed appropriately. Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Type of Action: Research and Innovation action

(c) [2018]: Digital security, privacy and personal data protection in finance

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

(1): Development of resilience enhancing technologies. Proposers are expected to develop innovative solutions tailored for the finance domain, ensuring that a proactive preparedness helps financial market participants and infrastructures to share information and better cope with technological shortfalls. Proposals should (i) deliver tools for making the exfiltration of data for attackers unattractive, both for ‘data at rest’ and 'data in transit'; (ii) consider incipient trends (e.g. digital on boarding based on biometric data); and (iii) collaborate with CERTs/CSIRTs.

(2): Development of new/enhanced, parameterized, automated and collaborative ICT tools for insurance companies, which are needed in order to collect security, privacy, personal data protection and accountability requirements from their clients and upgrade their insurance and liability policies respecting the EU legislation on cybersecurity, privacy and personal data protection, as well as cybersecurity standards (e.g. ISO27001, 27005).

(3): Standardization to allow the quick adoption of cybersecurity best practices in the domain. Applicants should propose novel solutions for promoting common standards for conducting stress and resilience testing across systemic financial market infrastructures and institutions or for certifying companies/organizations that can perform accredited conformity tests.

The outcome of the proposal is expected to lead to development up to Technology Readiness level (TRL) 7; please see Annex G of the General Annexes.

The Commission considers that proposals requesting a contribution from the EU of between EUR 3 and 4 million would allow this specific challenge to be addressed appropriately.

Nonetheless, this does not preclude submission and selection of proposals requesting other amounts.

Type of Action: Innovation action

Projects should also foresee activities and envisage resources for clustering with other projects funded under this topic and with other relevant projects in the field funded by H2020.

Expected Impact:

Short term:

- The technological and operational enablers of co-operation in Response and Recovery will contribute to the development of the CSIRT Network across the EU, which is one of the key targets of the NIS Directive.
- Identified relevant generic and specific aspects related to cybersecurity and digital privacy in the respective critical domains/sectors addressed.
- Advanced holistic systems and innovative proof concepts for managing cybersecurity and privacy risks in the respective critical domains/sectors addressed.
- Advances in the state-of-the-art analysis of specific aspects of the respective critical domains/sectors addressed, such as related cyber threats, attacks and vulnerabilities;
- Sound analysis of cascading effects of specific related cyber threats within the supply chain of the respective critical domains/sectors addressed.
- Improved cybersecurity information sharing and collaboration among stakeholders of the respective critical domains/sectors addressed, and with CERTs/CSIRTs.
- More targeted and acceptable security management solutions addressing specificities of the respective critical domains/sectors addressed.
- Trigger the fast adoption of cybersecurity/privacy/personal data protection best practices in the respective critical domains/sectors addressed.

Medium term:

- Better response and recovery technologies and services that will help organizations in the respective critical domains/sectors addressed to significantly reduce the impact of propagated and cascaded threats, vulnerabilities and breaches.
- Enhanced protection against emerging novel advanced threats in the respective critical sectors/domains addressed.
- Improved security governance of the respective critical domains/sectors addressed.

- Greater and more mature EU cybersecurity market in the respective critical domains/sectors addressed.
- Reduce the impact of breaches with various levels of success in penetrating the defences.

Long term:

- Better cybersecurity for specific standards in the respective critical domains/sectors addressed, that will trigger fast adoption of best practices in the related industry.
- Established trust chains among all entities in the eco-systems of the respective critical domains/sectors addressed.
- Better implementation of the relevant EU legislation (e.g. NIS, eIDAS, GDPR) in the respective critical domains/sectors addressed.
- Companies/organisations in the respective critical domains/sectors addressed are more willing to promote cyber security, privacy and personal data protection in the whole EU specific ecosystem.

Type of Action: Innovation action, Research and Innovation action

The conditions related to this topic are provided at the end of this call and in the General Annexes.

Conditions for the Call - Digital Security

Opening date(s), deadline(s), indicative budget(s):[60]

Topics (Type of Action)	Budgets (EUR million)			Deadlines
	2018	2019	2020	
Opening: 15 Mar 2018				
SU-DS01-2018 (IA)	16.00			23 Aug 2018
SU-DS04-2018-2020 (IA)	20.00 [61]			

[60] The Director-General responsible for the call may decide to open the call up to one month prior to or after the envisaged date(s) of opening.
The Director-General responsible may delay the deadline(s) by up to two months.
All deadlines are at 17.00.00 Brussels local time.
The deadline(s) in 2019 and 2020 are indicative and subject to separate financing decisions for 2019 and 2020.
The budget amounts for the 2018 budget are subject to the availability of the appropriations provided for in the draft budget for 2018 after the adoption of the budget 2018 by the budgetary authority or, if the budget is not adopted, as provided for in the system of provisional twelfths.
The budget amounts for the 2019 and 2020 budget are indicative and will be subject to separate financing decisions to cover the amounts to be allocated for 2019 and for 2020.

[61] of which EUR 5.00 million from the 'Secure, clean and efficient energy' WP part.

SU-DS05-2018-2019 (IA)	8.50			
Opening: 14 Mar 2019				
SU-DS03-2019-2020 (IA)		18.00		22 Aug 2019
SU-DS05-2018-2019 (RIA)		10.00		
SU-DS05-2018-2019 (IA)		10.00		
Opening: To be defined				
Focus area topic(s) for 2020			68.80 [62]	To be defined
Overall indicative budget	44.50	38.00	68.80	

Indicative timetable for evaluation and grant agreement signature:

For single stage procedure:

- Information on the outcome of the evaluation: Maximum 5 months from the final date for submission; and
- Indicative date for the signing of grant agreements: Maximum 8 months from the final date for submission.

Eligibility and admissibility conditions: The conditions are described in General Annexes B and C of the work programme.

Evaluation criteria, scoring and threshold: The criteria, scoring and threshold are described in General Annex H of the work programme.

Evaluation Procedure: The procedure for setting a priority order for proposals with the same score is given in General Annex H of the work programme.

The full evaluation procedure is described in the relevant guide published on the Participant Portal.

Consortium agreement:

All topics of this call	Members of consortium are required to conclude a consortium agreement prior to the signature of the grant agreement.

[62] of which EUR 15.00 million from the 'Secure, clean and efficient energy' WP part

SME instrument & Fast-Track-to-Innovation

The respective calls for the EIC-SME instrument call (H2020-EIC-SMEInst-2018-2020) and EIC-Fast-Track-to-Innovation (H2020-EIC-FTI-2018-2020) are found under the Horizon 2020 Work Programme Part – ***Towards the next EU Framework Programme for Research and Innovation: European Innovation Council (EIC) Pilot*** (part 17 of this work programme).

Other actions[63]

1. Reviews of projects

This action will support the use of appointed independent experts for the monitoring of actions (grant agreements, grant decisions, procurements, financial instruments).

Type of Action: Expert Contracts

Indicative budget: EUR 0.97 million from the 2018 budget(Review of projects) and EUR 0.74 million from the 2019 budget(Review of projects) and EUR 0.62 million from the 2020 budget(Review of projects)

2. Workshops, conferences, experts, communication activities, studies

- Organisation of an annual Security Research event.
- Support to workshops, expert groups, communications activities, or studies. Workshops are planned to be organised on various topics to involve end-users; preparation of information and communication materials, etc.
- Organisation of cybersecurity conferences and support to other cybersecurity events; socio-economic studies, impact analysis studies and studies to support the monitoring, evaluation and strategy definition for cybersecurity and digital privacy policy.

Type of Action: Public Procurement - null

Indicative timetable: First, second, third and fourth quarters of 2018, 2019 and 2020

Indicative budget: EUR 2.50 million from the 2018 budget(indicative number of contracts per year: 1 security research event, 2-4 workshop/communication activities/studies, 40-45 expert contracts, 3-5 in support to cybersecurity and/or digital privacy conferences/events/studies/policies/communication activities) and EUR 2.50 million from the 2019 budget(indicative number of contracts per year: 1 security research event, 2-4 workshop/communication activities/studies, 40-45 expert contracts, 3-5 in support to cybersecurity and/or digital privacy conferences/events/studies/policies/communication activities) and EUR 2.50 million from the 2020 budget(indicative number of contracts per year: 1 security research event, 2-4 workshop/communication activities/studies, 40-45 expert contracts, 3-5 in support to cybersecurity and/or digital privacy conferences/events/studies/policies/communication activities)

[63] The budget amounts for the 2018 budget are subject to the availability of the appropriations provided for in the draft budget for 2018 after the adoption of the budget 2018 by the budgetary authority or, if the budget is not adopted, as provided for in the system of provisional twelfths.
The budget amounts for the 2019 and 2020 budget are indicative and will be subject to separate financing decisions to cover the amounts to be allocated for 2019 and for 2020.

3. Space Surveillance and Tracking

Support to security aspects of Space Surveillance and Tracking.

The Decision No 541/2014/EU of the European Parliament and of the Council of 16 April 2014 establishes a Framework for Space Surveillance and Tracking Support (SST)[64].

The Consortium resulting from the implementation of the support framework for the emergence of an SST capacity at European level has established its own dedicated implementation structure in order to manage related Union support. Therefore support to SST under Horizon 2020 and other Union funding programmes should be entrusted to the above Consortium[65].

The option of full purchase costs of equipment, infrastructure or other assets could be included in the GA if/when duly justified, in conformity of "Article 6.2 D.2".

The identified beneficiary is the consortium resulting from the implementation of the SST support framework within the meaning of Article 7(3) of Decision No 541/2014/EU comprising entities designated by participating Member States[66,67] and the EU SATCEN[68,69].

The grant to identified beneficiary will be made in conjunction with the respective cumulative budget from the 'Leadership in Enabling and Industrial Technologies – Space' WP part, Copernicus and EGNSS.

Legal entities:

Consortium resulting from the implementation of the SST support framework within the meaning of Article 7(3) of Decision No 541/2014/EU comprising bodies designated by participating Member States under their responsibility and the EU SATCEN.

Type of Action: Grant to Identified beneficiary

---

64 OJ L 158 of 27 May 2014, p. 227–234

65 In line with recital 24 of the Decision No 541/2014/EU, article 129 of the Financial Regulation (Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council) and article 193 of its Rules of Application (Commission Delegated Regulation (EU) No 1268/2012) this action may be financed jointly from separate source programmes, namely Horizon 2020 Framework Programme (Regulation (EU) No 1291/2013 of the European Parliament and of the Council), the Copernicus programme (Regulation (EU) No 377/2014 of the European Parliament and of the Council) and the European Satellite Navigation programmes (Regulation (EU) No 1285/2013 of the European Parliament and of the Council).

66 http://ec.europa.eu/growth/sectors/space/security_en

67 Article 190(1)(d) RAP allows award of a grant without the call for proposals to "*[…] bodies designated by the Members States, under their responsibility, where those Member States are identified by a basic act as beneficiaries of a grant*".

68 Article 8 of Decision No 541/2014/EU: "*The European Union Satellite Centre (SATCEN) may cooperate with the consortium […]* ".

69 Article 190(1)(f) RAP provides for an additional exception to calls for proposals "*for actions with specific characteristics that require a particular type of body on account of its technical competence, its high degree of specialisation or its administrative power, on condition that the actions concerned do not fall within the scope of a call for proposals*."

Indicative timetable: Fourth quarter 2018, fourth quarter 2019 and fourth quarter 2020 respectively

Indicative budget: EUR 1.50 million from the 2018 budget(Space Surveillance and Tracking) and EUR 1.00 million from the 2019 budget(Space Surveillance and Tracking) and EUR 0.50 million from the 2020 budget(Space Surveillance and Tracking)

4. Pre-standardisation mechanisms for security[70]

Support to a consortium comprising CEN (coordinator) and CENELEC in cooperation with ETSI, as well as the JRC as the current ERNCIP coordinator, to address how to achieve timely standardization in the field of security, including through structural changes.

Pre-standardisation and standardisation processes as currently in place in the fields of security and civil protection are not considered satisfactory, whilst many of their components are very valuable: the JRC produces interesting pre-standards in cooperation with a broader research community; CEN/CENELEC and ETSI produce solid standards with the very active involvement of industry. However, both sets of activities are not very agile and they do not interface optimally.

These organizations are invited to propose mechanisms and novel ways of working and organizing themselves, towards the establishment of standardisation processes in the field of security that build upon the strength of the various processes in place, and increase their effectiveness, speed and efficiency.

Legal entities:

- Coordinator: European Committee for Standardization (CEN) - Brussels (Belgium)
- European Committee for Electrotechnical Standardization (CENELEC) - Brussels (Belgium)
- European Telecommunications Standards Institute (ETSI) - Valbonne (France)
- Joint Research Centre - Ispra (Italy)

This grant will be awarded without call for proposals in line with Article 190(1)(e) of the Rules of applications of Regulation (EU, Euratom) 966/2012, Regulation No 1268/2012 and Article 11(2) of the Rules for participation and dissemination in "Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020)", Regulation (EU) No 1290/2013.

Type of Action: Grant to Identified beneficiary

[70] This grant will be awarded without call for proposals in line with Article 190(1)(e) of the Rules of applications of Regulation (EU, Euratom) 966/2012, Regulation No 1268/2012 and Article 11(2) of the Rules for participation and dissemination in "Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020)", Regulation (EU) No 1290/2013.

Indicative budget: EUR 0.90 million from the 2018 budget(Pre-standardisation mechanisms)

CALLS and OTHER ACTIONS for 2020

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

H2020-SU-INFRA-2018-2019-2020[71]

Topic

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

Call - Security

H2020-SU-SEC-2018-2019-2020[72]

Topics

- Human factors, and social, societal, and organisational aspects for disaster-resilient societies [continued]
- Technologies for first responders [continued]
- Pre-normative research and demonstration for disaster-resilient societies [continued]
- Chemical, biological, radiological and nuclear (CBRN) cluster [continued]
- Human factors, and social, societal, and organisational aspects in fighting against crime and terrorism [continued]
- Technologies to enhance the fight against crime and terrorism [continued]
- Information and data stream management to fight against (cyber)crime and terrorism [continued]
- Explosives: detection, intelligence, forensics
- Human factors, and social, societal, and organisational aspects of border and external security [continued]
- Technologies to enhance of border and external security [continued]
- Demonstration of applied solutions to enhance border and external security [continued]

[71] This is the continuation of a call for which information is provided in the first section of this work programme part.

[72] This is the continuation of a call for which information is provided in the first section of this work programme part.

- Pan-European networks of practitioners and other actors in the field of security [continued]
- Strategic pre-commercial procurements of innovative, advanced systems to support security [continued]
- Pre-commercial procurements of innovative solutions to enhance security [continued]

Call - Digital Security

H2020-SU-DS-2018-2019-2020[73]

Topics

- Management of cyber-attacks and other risks
- Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises [continued]
- Cybersecurity in the Electrical Power and Energy Systems (EPES): an armour against cyber and privacy attacks [continued]

[73] This is the continuation of a call for which information is provided in the first section of this work programme part.

Budget[74]

	Budget line(s)	2018 Budget (EUR million)	2019 Budget (EUR million)	2020 Budget (EUR million)
Calls				
H2020-SU-INFRA-2018-2019-2020		24.00	38.00	18.00
	from 18.050301	*14.00*	*18.00*	*8.00*
	from 09.040303	*10.00*	*20.00*	*10.00*
H2020-SU-SEC-2018-2019-2020		138.20	156.36	185.00
	from 18.050301	*138.20*	*156.36*	*185.00*
H2020-SU-DS-2018-2019-2020		39.50[75]	38.00	53.80[76]
	from 09.040303	*39.50*	*38.00*	*53.80*
Contribution from this part to call H2020-EIC-FTI-2018-2020 under Part 17 of the work programme		3.87	3.87	3.87
	from 09.040303	*0.97*	*0.97*	*0.97*
	from 18.050301	*2.90*	*2.90*	*2.90*
Other actions				
Expert Contracts		0.97	0.74	0.62
	from	*0.68*	*0.50*	*0.40*

[74] The budget figures given in this table are rounded to two decimal places.
The budget amounts for the 2018 budget are subject to the availability of the appropriations provided for in the draft budget for 2018 after the adoption of the budget 2018 by the budgetary authority or, if the budget is not adopted, as provided for in the system of provisional twelfths.
The budget amounts for the 2019 and 2020 budget are indicative and will be subject to separate financing decisions to cover the amounts to be allocated for 2019 and for 2020.

[75] To which EUR 5.00 million from the 'Secure, clean and efficient energy' WP part will be added making a total of EUR 44.50 million for this call.

[76] To which EUR 15.00 million from the 'Secure, clean and efficient energy' WP part will be added making a total of EUR 68.80 million for this call.

	18.050301			
	from 09.040303	*0.29*	*0.24*	*0.22*
Public Procurement		2.50	2.50	2.50
	from 09.040303	*0.50*	*0.50*	*0.50*
	from 18.050301	*2.00*	*2.00*	*2.00*
Grant to Identified beneficiary		2.40	1.00	0.50
	from 18.050301	*2.40*	*1.00*	*0.50*
Estimated total budget		211.44	240.47	264.29