Scoping Paper for

Horizon 2020 work programme 2018-2020

Societal Challenge 7: Secure societies – Protecting freedom and security of Europe and its citizens

Important Notice: Working Document

This scoping paper will guide the preparation of the work programme itself. It is a working document not formally endorsed by the Commission, and its content does not in any way prejudge the final decision of the Commission on the work programme.

The adoption and the publication of the work programme by the Commission are expected in October 2017. Only the adopted work programme will have legal value.

Scoping paper for the Horizon 2020 work programme 2018-2020
Societal Challenge 7: Secure societies – Protecting freedom and security of Europe and its citizens

1. Context

The European Agenda for Security sets out how the European Union can contribute, including through security research, to ensuring more secure societies. Much work is underway to strengthen the EU-wide security framework, with greater cooperation and data exchange across national boundaries. An issue is to provide security practitioners, public and private organisations, operators of critical infrastructure, as well as SMEs, with access to technological enablers, and innovative organizational measures, for the security capabilities that they need. Individual citizens also in particular need tools to deal better with cyber-attacks and to protect their personal data and privacy.

The Horizon 2020 "Secure Societies" challenge represents by far the most significant source of research funding in Europe for developing security technology, strengthening practitioner capabilities and increasing the competitiveness of the European security industry. Some actions lead to results that are classified information. Other results are of general interest and can be openly disseminated.

The "Protection And Security Advisory Group" (PASAG) is the major source of inspiration for this paper. There has also been input from EU Member State administrations, civil society organisations through the SecurePART FP7 project, security-related networks (e.g. ENLETS, ENFSI, EFRIM, RAN) and associations of research organisations (e.g. EARTO, IGLO) or of industries (e.g. ASD, EOS), as well as from the cPPP Strategic Research and Innovation Agenda on Cybersecurity and Digital Privacy and the CONNECT Advisory Forum. The following conclusions result from those consultations:

Build on steps already taken to involve practitioners: This will help industry, academia and research centres grasp the needs of end-users and encourage practitioners and industry to take ownership of outcomes. It will help practitioners better understand the benefits of planning for the longer term, both in terms of aspirational security solutions and the technology roadmaps necessary to achieve them. It will also increase interaction and cooperation between Member State institutions. EU support to knowledge networks adds value by knitting together EU-wide communities of interest.

Encourage and support a network of security practitioners and first responders: This will help disseminate best practices and the outcomes of innovation and research actions, and consequently enable more effective responses to crises. Such a network could also function as a knowledge hub (e.g. on lessons learned) so as to increase resilience and improve response capacities.

Design Calls to adapt research priorities to changing circumstances: Crime, terrorism and natural catastrophes are not always predictable. The "Secure Societies" challenge provides the

underpinning for developing Europe's security capability, and as such it must be quick to adjust to circumstances.

Reduce barriers to cross-border cooperation – of Member States, industry and practitioners – which are higher-than-average in the security field: Research output will continue to be made available at fair, reasonable and non-discriminatory terms. Support to European standardization activities will help ensure that solutions can be used across borders without the need for specific local adaptations.

Expand collaboration between the public and private sectors: The public-private partnership (PPP) on cybersecurity will continue. Other models to encourage developing market-oriented and affordable solutions should be tested in order to reduce costs for operators by transferring to the private sector the responsibility to acquire and operate capability. Where possible, EU Agencies will be involved. Innovation actions aimed at demonstrations and pre-commercial procurement should be considered.

Investment in security should not be addressed exclusively within the "Secure Societies" challenge: Security crosses into other Horizon 2020 activities. ICT, Transport, Energy, Climate action and Space are some areas where security needs to be built into the design of new solutions and where cross-border impacts have important security implications. Closer coordination within an Horizon 2020 "Boosting the effectiveness of the Security Union Focus Area" will ensure that such security implications are properly considered.

2. Strategic orientations for 2018-2020 and translation into calls

Five key areas of activity have been identified for the forthcoming funding periods:

i) Borders and External security

ii) Fighting Crime and Counter-terrorism

iii) Secure and Resilient Societies

iv) Cybersecurity and Digital Privacy

v) Competitive European Security Industry

For each a "vision" for 2030 has been prepared, to ensure that what gets funded in 2018-2020 represents stepping stones along a roadmap to deliver the vision, taking account of the main challenges ahead, of research, development and innovation (RDI) milestones, of new markets that may develop and the emergent technologies that may disrupt or induce paradigm changes.

2.i) Borders and External security

In 2030 EU citizens should be able to cross land, sea and air, internal and external EU borders, with no physical barriers; Goods will be monitored through innovative techniques that require neither interrupting or constraining traffic flows nor visual inspection; Controls will be by exception and triggered by alerts activated throughout the EU and not exclusively at the border; Non-EU citizens and goods will be subject to a single EU-wide entry protocol,

while their intra-EU movement will be monitored through the same interface applicable to EU citizens and goods when within the EU.

Main challenges: Achieving integrated border management through a common interface (common to air, land or sea; people or cargo; transportation modes); Developing a comprehensive border technology roadmap within an established EU border control strategy; Coordinating border security with comprehensive immigration and border management policies, including privacy and civil rights implications; Implementing planning, coordination and information-sharing among national and EU border security authorities and practitioners; Transitioning to service-oriented PPPs.

RDI milestones will set goals within technology roadmaps, to be established in cooperation between industry and practitioners, e.g.: Systems tools, and methods for rapid identification for both control and surveillance, exploring the potential of EUROSUR and CISE and promoting new technology; Holistic systems to support the EU's external security in civilian tasks (e.g. humanitarian relief, border management, peace-keeping and post-crisis stabilisation); Innovative business models to enable new private sector services to augment border management capability. Demonstrators meeting practitioners' requirements and implementing state-of-the-art capabilities will be required.

Emerging/disruptive technologies may include: AI-embedded autonomous systems (e.g. drones to patrol borders); Web intelligence; Big data; Processing, fusion and visualisation tools; Real-time stand-off liquid explosives detection; Multi-spectral sensing and miniaturisation of sensors.

New markets may emerge: Advanced security products accessible throughout the EU; 'Big data' solutions and human-machine interfaces; IT systems integrating legacy and new systems across multiple countries; Private sector provision of border management capabilities.

2.ii) Fighting crime and counter-terrorism

In 2030 EU citizens and residents in good standing should be able to live and operate in peace and freedom, including in the digital environment. As crime and terrorism continue to evolve from local to international, and from socially-connected groups to virtually-connected anonymous networks, there should be increased capabilities to predict, monitor, recognise and prevent them, and faster or real-time responses with improved exploitation of advanced digital tools as well as metadata and social engineering, including community of interest groups created to protect their members. Law enforcement will meet new behavioural and technological challenges including in encryption and privacy protection, to detect, investigate and prevent criminal activity. Technological advances will make evidence more robust thus enabling reactive, efficient and fair justice systems.

Main challenges: Understanding the threats, given their evolving and more international nature; Understanding causes and impacts of radicalisation, violent extremism and terrorist beliefs; Studying those phenomena, and creating and testing anti-radicalisation measures, producing evidence-based tools and policy recommendations for both policy-makers and law

enforcement agencies, including Member States' security practitioners, and directly involving the Radicalisation Awareness Network (RAN) to bridge the gap between academia and security practitioners; Understand differences in national approaches, better to adapt best practices and research outcomes to local conditions. Another challenge will be to address the rising role of new technologies in organised crime and trafficking activities (e.g. crypto-currencies, online markets and open access to information on drugs, firearms and other illegal products, counterfeit medicines).

RDI milestones may include: Web tools to monitor organised crime; Automating analysis of digital evidence (e.g. to identify faster victims of child sexual abuse and to disrupt the availability of such material online); 'Big data' analytics based on open source technology; Predictive analytics; European standards for exchanging information, evidence and best practices between law enforcement agencies; Novel technologies to reduce the use of force by law enforcement agencies.

Emerging/disruptive technologies may include: Quantum computing (e.g. for decryption); Artificial Intelligence; Nanotechnology, as well as Augmented Reality and Virtual Reality in investigation techniques; Autonomous systems (e.g. robots, drones) for use in enforcement and detection.

New markets will emerge: Private security services for both public and private domains; Cybersecurity and cyber assurance.

2.iii) Secure and Resilient Societies

In 2030 European society, government and commerce should be more resilient to malicious, natural and accidental disruption despite increasing dependence on interconnected ICT infrastructure and ever more risks and threats. Critical national and EU infrastructures will be resistant to attack by physical and cyber means, and will continue to operate, even under the most severe scenarios, with minimal societal impact. Security and resilience will be coordinated at all levels of society. Disaster relief agencies and first responders will be well-equipped, effective and cooperate well across borders. Citizens and companies will accept that laws and policies to protect society respect individual rights and freedoms, and have trust in the institutions that implement them. All parts of society will be fully engaged and valued regardless of gender, ethnicity, religion and wealth. A wide selection of affordable and trusted security and resilience products and services will be available.

Main challenges: Coping with the complexity and diversity within European society, and to limit its exposure to risk from a variety of natural, accidental, political, economic and malicious threats. This includes addressing questions of national and transnational vulnerabilities, resilience and capabilities related to prevention, preparedness, response and recovery. This requires identifying high-priority threats, protections and counter-measures as well as developing and validating models and principles regarding the kinetic response and disaster resilience of society at large; the resilience of organisations and infrastructure; and human factors and societal resilience to disaster and insecurity.

RDI milestones will include: Innovative methods and tools to highlight best practice and strengthen cross-border interoperability of first responders; Integrated and interconnected systems and tools for operational use; Innovative guidelines for designing, constructing and managing secure and resilient organisations and social systems; Serious gaming; Identification of the key features and tipping characteristics of the trusted institutions and services underpinning resilient societies; Innovative methods to motivate and empower communities to contribute to security and resilience; Innovative guidelines for designing institutions for governance of security and resilience of societies; Ways to detect societal vulnerabilities; Testing of such methods, tools, and systems.

Emerging/disruptive technologies may include: Blockchain to support decentralised institutions; Fully autonomous, intelligent systems (e.g. robots, drones, sensors) for use in detection and response; Gaming technologies integrated into social media/networks.

New markets may include innovative information and simulation services.

2.iv) Cybersecurity and Digital Privacy

In 2030 cybersecurity and privacy technologies should become complementary enablers of the European digital economy, ensuring a secure and trusted networked environment for governments, businesses and individuals, positioning the EU as a world leader in building a more secure digital economy. European citizens and organisations will benefit from user-friendly cybersecurity and privacy systems enabling them to be active participants in their own security.

The main challenges and how to address them are addressed in the July 2016 Communication on strengthening cyber-resilience and fostering the cybersecurity industry. Cybersecurity and digital privacy are relevant to almost all areas of economic and social activity; relevant R&I thus spans beyond "Secure Societies" into LEIT ICT and other Societal Challenges. Challenges include assuring cybersecurity and privacy in the design and management of networks, while taking account of needs of law enforcement and judicial investigation; achieving a high degree of trust in EU digital networks, products and services as a key value and competitive advantage of the EU; developing the ecosystem of skilled professionals, educators and EU-wide harmonized regulation, policies and standards.

RDI milestones will include: Assurance and security/privacy by design; Identity, access and trust management; Data; ICT infrastructure cybersecurity; Cybersecurity services.

Cybersecurity has grown to encompass all aspects of technological, social, economic and political life. Specific research topics should therefore be complemented by multidisciplinary research on longer term cybersecurity paradigms and challenges, addressing non-technical aspects of cybersecurity and digital privacy such as economics and law as well as political science and international relations.

The Cybersecurity contractual Public Private Partnership established in 2016, which aims to build trust among Member States and industry by fostering cooperation at early stages of the

research and innovation process and to help align demand and supply, will draw heavily from WP2018-20 of Horizon 2020. It will facilitate the engagement of end-users in sectors that are important customers of cybersecurity solutions (e.g. energy, health, transport, finance) towards defining and providing to industry their sector-specific common digital security, privacy and data protection requirements.

2.v) A competitive European security industry

In 2030 the European security industry will be key to creating a secure operating environment for EU governments, businesses and the public in a digitally connected global market; A more integrated European Security ecosystem underpinned by recognition and trust will be achieved through strategies to connect supply and demand sides of markets; This ecosystem's shared knowledge base will be enhanced by networks linking innovation paths of mutual interest, making non-sensitive information rapidly available, and generating significant wealth including through small agile companies alongside established businesses and multi-national corporations; There will be a single market for security products, systems and services, supported by standards based on European leading technologies together with efficient testing, auditing and conformity assessment.

Main challenges: Supporting a digitally connected global market underpinned by European standards defined jointly by industry and operators/users; Agreeing with Member States a shift from national requirements and controls to EU-level standardisation (including possible certification) for security products and services, so as to facilitate at affordable costs; Reducing the fragmentation of the European market where this hinders the emergence of pan-European and global operators.

RDI milestones will include: Setting up networks, test beds, EU "clusters" of industry and users, security "centres of excellence", and a Market Analysis Observatory open to EU industry and users; Protocols for data exchange and for interface with space technology; Creating funding instruments for exploiting new technologies, especially by SMEs; Creating a Scientific, Ethics and Business advisory group on, inter alia, the balance between collective security and privacy technologies.

Emerging/disruptive technologies may include: Internet of Everything; Big data; Artificial Intelligence; New materials (e.g. graphene); Virtual reality for simulation; Miniaturisation; Synthetic biology.

New markets may include smart personal protective equipment (e.g. wearables, female body armour); Secure and faster delivery for E-commerce.

3. Cross-cutting issues

The role of the individual in society: It is individuals, not society, that e.g. cross borders, and individuals value freedom and privacy in ways that may contradict security best practices. We need to preserve these fundamental values while assuring an adequate collective security. Similarly, individual creativity and enterprise can be significantly leveraged by digital networks to the benefit of society, but network security must take account of the rights of

individuals. The human factor will remain at the centre of the "Secure Societies" challenge, which will also consider new approaches in areas such as social networks to deepen engagement within sections of society, to promote community awareness, and to develop the role of communities in crisis readiness and management.

Gender: In the area of Borders and Security, gender impacts on the nature of flows of people, immigration and border control. As for Fighting Crime and Counter-terrorism, gender is relevant in relation to perpetrators and victims of crime and terrorism. A specific focus might be international gender dimensions of radicalisation, including women's roles in countering violent extremism. Gender is relevant to people trafficking, both of those controlling it and its victims. Resilience needs to understand different ways of engaging, and assessing impacts on, the different genders; this may lead to new approaches in areas such as community awareness and crisis readiness. Cybersecurity will need to take account of gender in developing more user-friendly and accessible security systems.

International cooperation: Pros and cons for international cooperation targeting specific partner countries will be assessed on a topic-by-topic basis.

4. Calls

Call working title	*Brief description of the scope*	*Possible contribution from and to other work programme parts (mandatory only for focus area calls)*
Addressing combined kinetic and digital threats	Protection of Critical Infrastructure.	n/a
Boosting the effectiveness of the Security Union	Topics under areas i, ii, iii, iv, v (to be defined) and parts of LEIT ICT, LEIT Space, SC6 (inclusive societies), SC4 (transport)	€700-750 million from SC7, LEIT Space, LEIT ICT, SC6 and SC4 *(see separate note on the "Boosting the effectiveness of the Security Union Focus Area")*
Fight against Crime and Terrorism, Disaster Resilience, Border and External Security	Topics under areas i, ii, iii, v, not covered by the virtual focus area	n/a
Cybersecurity and Digital Privacy	Topics under area iv, not covered by the focus area; strong complementarity with LEIT ICT and other Societal Challenges addressing these issues	n/a