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

1. Context

The European Agenda for Security is setting the pace for European Union activities towards more secure societies, and it refers to security research. Much work is already underway at European level to strengthen the EU-wide security framework, with greater co-operation and data exchanges 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 the technological enablers, and innovative organizational measures, for the capabilities they need with regard to security – including cybersecurity. Individual citizens also need the right tools to better prevent, detect, respond to and recover from cybersecurity attacks as well as protect their personal data and privacy.

The Horizon 2020 "Secure Societies" challenge represents by far the most significant source of funding in Europe for the development of security technology and solutions to strengthen practitioner capabilities and the competitiveness of the European security industry. It supports some sensitive actions in which participants need to manage classified information. Other actions produce results of general interest, which can be openly disseminated.

The "Protection And Security Advisory Group" (PASAG) has been the major source of inspiration for this scoping paper. It has been complemented with interaction and input gathered from some EU Member State administrations, civil society organisations through the SecurePART FP7 project, security-related networks (ENLETS, ENFSI, EFRIM, RAN, etc.) and associations of research organisations (e.g. EARTO, IGLO) or of industries (e.g. ASD, EOS), as well as with guidance proposed in the cPPP Strategic Research and Innovation Agenda on Cybersecurity and Digital Privacy, and the Connect Advisory Forum paper on Cybersecurity.

The following conclusions result from PASAG and stakeholder consultations:

Build on the steps already taken to achieve greater involvement of practitioners in the research and innovation actions: It will help industry, academia and research centres grasp the real-life requirements of the end-users and encouraging practitioners and industry to take ownership of the outcomes. It will also help practitioners gain a greater appreciation of the benefits of planning for the longer term, both in terms of aspirational security solutions and the respective technology road maps necessary to achieve them. It will also lead to greater interaction and closer cooperation between Member State (MS) institutions. EU support to knowledge networks adds value by knitting together EU-wide communities of interest.

Encourage and support an effective and functioning network of security practitioners and first responders: They will contribute disseminating best practices and the outcomes of innovation and research actions, and consequently, enable a more effective, real-time institutional response to crises. Such networks could also function as knowledge hubs that maintain 'organisational

knowledge' for instance in the form of lessons learned to further increase resilience & further improve response capacities.

Design Calls to adapt research priorities to changing circumstances: Crime, terrorism and natural catastrophes do not conform to a predictable view of events and consequent policy responses. Innovation is a constant requirement. Where the "Secure Societies" challenge provides the underpinning for Europe's security capability development, it must be quick to adjust to circumstances and continue to stay relevant.

Reduce the barriers to cross-border co-operation – of Member States, of industry and of practitioners – which are notably higher-than-average in the field of security: Special programme modalities which provide that research output will be made available at Fair, Reasonable and Non-discriminatory terms will be continued. Support to European standardization-related work will continue to help ensure that security solutions can be applied across borders without the need for specific adaptations to local requirements.

Collaboration between the public and private sectors in the field of civil security need to be expanded: The public private partnership (PPP) on cybersecurity is to continue. Other models that encourage the development of market-oriented, affordable and practical solutions should also be tested to alleviate the acquisition burdens of the operators, by transferring the responsibility to acquire and operate capability to the private sector. Where possible, EU Agencies will be involved. Innovation actions aimed at demonstrations and pre-commercial procurements are instruments to be considered.

Investment in security capabilities should not be addressed exclusively within the "Secure Societies" challenge: Security is inherent to many other sectors of society and crosses into other Horizon 2020 activities. ICT, Transport, Energy, Climate action and Space are just a few areas where Security needs to be built into the design of new solutions and capabilities and where the cross-border impact has important security implications. Closer coordination within an Horizon 2020 "Virtual Focus Area" will ensure that security implications are properly considered and complement the initiatives launched under the "Secure Societies" challenge.

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

Five key focus domains 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 delivering tomorrow's 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 all land, sea and air, internal and external EU borders, with no physical barriers; Goods and freight will be monitored through innovative techniques that will not require interrupting, channelling or constraining traffic flows or visual inspection; Controls will be exercised by exception and be triggered by alerts activated throughout the EU and not exclusively at border crossings; Non-EU citizens and goods will be subjected to a single EU-wide entry protocol and monitoring of their intra-EU movement will be effected through the same network interface applicable to EU citizens and goods, when within EU territory.

Main challenges consist in 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 and co-ordinating border security with comprehensive immigration and border management policies, including privacy and civil rights implications; Implementing planning, co-ordination and info-sharing among national and EU border security authorities and practitioners; Transitioning to service-oriented PPPs.

R&D&I milestones will pave technology investment road maps, to be established in co-operation between industry and practitioners: Systems, equipment, tools, processes and methods for rapid identification for both control and surveillance issues, exploring the potential of EUROSUR and CISE and promoting new technology for border checks; Holistic systems to support the EU's external security in civilian tasks (civil protection, humanitarian relief, border management, peace-keeping and post-crisis stabilisation); Innovative business models to enable new private sector services to augment border management capability including airborne and land-based surveillance. Demonstrators involving industry and end-users, meeting practitioners' requirements, and evaluating and implementing state-of-the-art capabilities will be required.

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

New markets may emerge: Advanced security products accessible throughout the EU; 'Big data' solutions and man-machine interfaces; IT systems integrating legacy and new systems across multiple countries; Private sector ownership of assets and service 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 localised to international, and from socially-connected groups to virtually-connected anonymous networks, efforts should be made to increase the capability of predicting, monitoring, recognising and preventing them will also increase, and more, 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 focus on meeting 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 will include: Understanding the threats to EU citizens and organisations, given their rapidly evolving and more international nature; Understanding causes and impacts of radicalisation, violent extremism, terrorist ideas and beliefs to reduce related threats, studying the phenomenon and setting up, experimenting and assessing anti-radicalisation measures and policies, producing science-based tools and providing policy recommendations actionable by both security policy-makers and law enforcement agencies, including security services in the Member States, and with the direct involvement of the Radicalisation Awareness Network (RAN) to effectively bridge the gap between academia and security practitioners; The differences in national laws and approaches, to better adapt best practices and research outcomes to local conditions and requirements. Increasing use of open source technology by public services may hinder innovation by industry which prefers commercially proprietary technology A challenge will also be to cope with the criminal abuse of emerging technologies (e.g. crypto-currencies), or protecting citizens' privacy, with law enforcement access to evidence. Another challenge will be to address the rising role of new technologies on organised crime and trafficking activities (online markets and open access to information on drugs, counterfeits medicines, firearms and other illegal products);

R&D&I milestones will include: The development of web monitoring tools on organised crime; The automation of analysis of digital evidence (e.g., to identify faster victims of child sexual abuse and disrupt the availability of child sexual abuse material online);; 'Big data' analytics based on open source technology , with tools to handle, analyse and visualise large amounts of data; Predictive analytics;; European standards for exchanging information, evidence and best practices between law enforcement services and agencies; Novel technologies to reduce the use of force by enforcement agencies.

Emerging/disruptive technologies may include: Quantum computing (e.g. for decryption); Artificial Intelligence; Use of nanotechnology, as well as AR and VR in investigation techniques; Autonomous systems (e.g. robots, UAVs) for use in enforcement and detection; crime dedicated malware.

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, and the services they depend on should be more resilient to malicious, natural and accidental disruption despite increasing dependence on interconnected ICT infrastructure, and the existence of an ever more varied set of risks and threats. Public and private sector 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. There will be co-ordination and co-operation on security and resilience at all levels of society. Disaster relief agencies and first responders will be well-equipped and effective and co-operate well across national borders. Citizens and companies will accept that the laws and policies to

protect society balance collective security and individual rights and freedoms, and have trust in the institutions that implement and enforce them. All communities and segments of society will be fully engaged and valued regardless of gender, ethnicity, religion and financial status. A wide selection of effective, affordable, compatible and trusted security and resilience products and services will be available.

Main challenges will be to cope with the complexity and diversity within the European society, at 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, after having identified high-priority threats, protections and counter-measures and also developed, and validated models and principles regarding:

- kinetic response and disaster resilience of the society at large;
- resilience of organisations and infrastructure;
- human factors and societal resilience to disaster and insecurity.

R&D&I milestones will include: Innovative guidelines, 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 under-pinning secure and resilient societies; Innovative methods to motivate and empower communities to contribute to security and resilience; Innovative guidelines for the design of institutions for governance of security and resilience aspects of societies; Solutions for the detection of societal vulnerabilities; Fully fledged experimentation of such guidelines, methods, tools, techniques and systems.

Emerging/disruptive technologies may include: Block-chain to support decentralised institutions; Fully autonomous, intelligent systems (e.g. robots, UAVs, 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 mutually supportive and 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 safer and more secure digital economy. European citizens and organisations will benefit from user-friendly and accessible cybersecurity and privacy systems enabling them to be active participants in safeguarding the resilience of the digital economy. Citizens will increasingly move from being users of digital interfaces to informed participants in their own security.

The challenges Europe faces in regards to cybersecurity and how to better address them are the subject of the recently published Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry. Cybersecurity and Digital Privacy challenges that span across ICT technologies and are relevant to almost all areas of economic and

social activity need to be addressed both in the design of systems as well as with appropriate tools and services that can counter cybersecurity and privacy threats. Cybersecurity and Digital Privacy R&I therefore spans beyond SC7 into LEIT-ICT as well as other Societal Challenges. Challenges also include assurance of cybersecurity and the fundamental right to privacy at the very centre of design, management and control of ICT networks, while maintaining a balance between individual privacy/freedom and enforcement and judicial investigation; achieving a high degree of trust in EU digital networks, systems, products and services as a key value of the EU and develop it into a competitive advantage; developing the ecosystem of skilled professionals, educators and EU-wide harmonized regulation, policies and standards.

Specific R&D&I milestones will include: Assurance and security/privacy by design; Identity, access and trust management (Identity and Access Management, Trust Management); Data security (and encryption); ICT Infrastructure Cybersecurity (Cyber Threats Management, Network Security, System Security, Cloud Security, Trusted hardware/ end point security/ mobile security); Cybersecurity services (Auditing, compliance and certification, risk Management, cybersecurity operation centres, security training services).

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

The Cybersecurity contractual Public Private Partnership established in 2016, which aims to build trust among Member States and industrial by fostering cooperation at early stages of the research and innovation process, and to help align the demand and supply sectors 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 safe and 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 has been achieved through strategies to connect effectively supply and demand sides of the markets; The shared knowledge base of this ecosystem is enhanced through networks linking innovation paths of mutual interest, making non sensitive information available on a rapid basis, and generating significant wealth including through the combination of small agile companies with more established businesses and multi-national corporations; The industry operates within an integrated single market supported by standards based on European leading technologies, together with efficient testing, auditing and conformity assessment of security products, systems and services.

Main challenges will include: Supporting a digitally connected Global Market underpinned by the development of European standards, defined jointly by industry and operators/users; Negotiating within the EU for the Member States to relinquish national controls and requirements on standards

for security and security products, not to hamper practitioners' ability to innovate at affordable costs and allow standardisation (including possible certification) at the EU level; Reducing the fragmentation of the European market, where it hinders the emergence of pan-European and global operators.

R&D&I milestones will include: The establishment of networks, test beds, EU-based "clusters" of industry and operators/users, security "centres of excellence" in EU universities/research institutes/companies, a Market Analysis Observatory open to EU industry, SMEs, and individual users; Protocols for data exchange and for interface with space technology; The creation of new funding instruments for exploitation of new technologies, especially by SMEs; The establishment of a Scientific, Ethics and Business advisory group on, inter alia, the balance between collective security and privacy technologies.

Emerging/disruptive technologies may include: IoE - 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**

Societal concerns and issues of a crosscutting nature will influence the work-programmes of the "Secure Societies" challenge:

The role of the individual in society: For example, individuals, not society, cross borders for legitimate or improper motivations; and individuals value their freedom and their privacy, in ways that may contradict security best practices. We need to understand and preserve these fundamental values while assuring and instilling an adequate and supported level of collective security. Similarly, individual creativity, learning and enterprise can be significantly leveraged by digital networks to the great benefit of society, but their security can only be assured in a way which is mindful not only of society but of the rights and objections of the individual. The human factor will be maintained at the centre of the "Secure Societies" challenge, which will also consider new approaches in areas such as social networks, supported by social media, 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 strategies, instruments and processes of counter-terrorism. A specific focus might be the international gender dimensions of radicalization and counter-radicalization including women's roles in preventing and countering violent extremism. Gender is also relevant to trafficking of goods and people both of those controlling it as well as those who are victims. Resilience needs to take account of gender through understanding of different ways of engaging, and assessing the impact on, different groups in society, which will offer possibilities for new approaches and strategies in areas such as community awareness, crisis readiness and

management. Cyber-security will need to take account of gender in developing more user-friendly and accessible security systems.

International co-operation: Pros and cons for international co-operation 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	To be defined	n/a
Security Virtual Focus Area	Covering topics under areas i, ii, iii, iv, v (to be defined) and parts of LEIT ICT, LEIT Space, SC5 (climate change), SC4 (transport security)	700-750 million € from SC7, LEIT Space, LEIT ICT, SC5 and SC4 *(see separate note on the "Security Virtual Focus Area")*
Fight against Crime and Terrorism, Disaster Resilience, Border and External Security	Covering topics under areas i, ii, iii, v, not covered by the virtual focus area	n/a
Cybersecurity and Digital Privacy	Covering topics under areas iv, not covered by the virtual focus area; strong complementarity with LEIT-ICT and other Societal Challenges addressing these issues	n/a