

Scoping Paper for

Horizon 2020 Societal Challenge 'Secure Societies - protecting freedom and security of Europe and its citizens'

Important Notice: Working Document

This paper is a working document. It is sent to the Programme Committee for the Horizon 2020 Specific Programme for discussion in the context of the preparation of the Horizon 2020 Work Programme 2016-2017. As such, information and descriptions of activities indicated in this document may not appear in the adopted Work Programme 2016-2017, and likewise, new elements may be introduced.

1. Context

The development process of this scoping paper:

This draft scoping paper is based primarily on the report prepared by the Horizon 2020 Secure Societies Advisory Group. The Advisory Group is composed of representatives from all relevant stakeholder groups, i.e.: public end-users, research organisations, academia, small and large industry, and non-governmental organisations. Additionally, several specific key external stakeholders have provided their own views on the scope of the Secure Societies Work Programme 2016-2017:

- Integrated Mission Group for Security (IMGS)
- European Network of Law Enforcement Technology Services (ENLETS)
- European Organisation for Security (EOS)
- AeroSpace and Defence (ASD)
- The Network and Information Security Public-Private Platform (NIS-P)
- The Trust in Digital Life community (TDL)

Policy objectives:

The aim of the “Secure Societies - protecting freedom and security of Europe and its citizens” challenge is to support the implementation of EU policy initiatives on security matters and the competitiveness of the security industry, as a contribution to the new Commission’s agenda for “A New Boost for Jobs, Growth and Investment”, and taking into account the Security Industry Policy¹.

The “Secure Societies” challenge will also contribute to additional priorities of the Political Guidelines for the new European Commission, such as making the European Union:

A Connected Digital Single Market

ICT-driven transformations bring opportunities across many important sectors but also vulnerabilities to critical infrastructures and services, which can have significant consequences on the functioning of society, economic growth and the technological innovation potential of Europe. Such security-related issues will be addressed with the “Digital Security” call.

A Stronger Global Actor...

¹ COM(2012)417 final

The “Border and External Security” call will support the introduction of innovative technologies and processes in how the Union implements its External Security policies.

... Towards a New Policy on Migration

The “Border and External Security” call will support the introduction of innovative technologies and processes in the border control authorities’ efforts to secure the EU external borders, fight against human traffickers, whilst facilitating the legitimate flow of people and of goods and rescue lives of migrants at risk.

An Area of Justice and Fundamental Rights Based on Mutual Trust

The calls “Fight against crime and terrorism”, “Privacy” and “Ethics” will support the development of new technologies and innovation in capabilities for fighting and preventing crime (including cyber-crime), illegal trafficking, and terrorism (including cyber-terrorism), and for better understanding and tackling terrorist ideas and beliefs, while guaranteeing fundamental rights and values, including procedural rights and the protection of personal data.

The Secure Societies Work Programme 2016-2017 will directly contribute to the implementation of the current European Internal Security Strategy², the Security Industrial Policy³, and the Cyber Security Strategy⁴.

Areas already covered in the previous work programme 2014-2015:

The actions resulting from the Work Programme 2014-2015 are to enhance the resilience of our society against natural and man-made disasters, ranging from new crisis management tools to communication interoperability, to develop novel solutions for the protection of critical infrastructure (call 1); to fight crime and terrorism ranging from new forensic tools to protection against explosives (call 2); to improve border security, ranging from improved maritime border protection to supply chain security and to support the Unions external security policies including through conflict prevention and peace building (call 3); and to provide enhanced cybersecurity (call 4), ranging from secure information sharing to new assurance models.

2. Strategic orientations for 2016-2017

2.1. Continuity

The general feedback received so far has been positive, as shown by the good participation in the 2014 calls (with a tenfold oversubscription). All four calls have been well received by the security research stakeholders, who participated heavily across the board and expressed their support for a strong element of continuity in planning for 2016-2017. The following calls will therefore be maintained:

2.1.1. Disaster Resilient Societies

Owing to the growing risk of man-made and natural disasters resulting from increasingly frequent and severe natural and man-made hazards, and to the increasingly cross-sectorial and cross-border dimension of these risks resulting from the complex interdependence of sectors in our society, the security of citizens, infrastructure and assets has become a high priority in the European Union and beyond. It is only by working together on European solutions that the EU

² COM(2010) 673 final

³ COM(2012)417 final

⁴ JOIN(2013)1 final

will be able to overcome the impact of earthquakes, floods or forest fires, pandemics and other chemical and environmental health threats that often affect series of neighbouring countries and that cannot be resolved by individual Member States. In this respect, research developments in the areas of Chemical, Biological, Radiological, Nuclear and Explosives, critical infrastructure protection, risk assessments and natural and man-made disaster management remains essential.

Three Coordination and Support Actions (CSA) are being launched in 2014-2015, which may be worth continuing with a next logical phase: for strengthening capacity building for health and security in case of large pandemics in a World without borders (demonstration project following-up DRS4), developing a downstream activities (Pre-Commercial procurement or Public Procurement of Innovative Solutions) dealing with Civil Protection decision-making solutions (follow-up of DRS5) and launching a Pre-Commercial procurement or a Public Procurement of Innovative Solutions on the next generation of interoperable secure communication technologies (follow-up of DRS18). The SME instrument related to the protection of urban soft targets (follow-up of DRS17) could also be continued since urban security remains an issue of importance, and an area prone for SME involvement.

Further to the above-listed “legacy” actions from the Work Programme 2014-2015, the scope of the area could remain as is and described in a more general way. A few additional domains were highlighted during discussions with stakeholders that could be also usefully covered in the next work programme:

- In food security research in particular as regards traceability of toxic contaminants, from manufacturing to packaging;
- In line with the 2014 EU Maritime Security Strategy, research related to the expected impact of the opening of new routes and the increase of human activity in the polar region/Arctic in terms of disaster resilience and crisis management;
- Research on risk assessment methodologies and tools in particular as regards multi-hazard and cross-border risks in Europe and beyond;
- Research on the cascading effects of failure of a critical infrastructure on interdependent systems and the economy/society at large;
- In pre-normative research: on technologies to facilitate disaster recovery operations; on quality assurance of Chemical, Biological, Radiological, Nuclear and Explosives measurements.

Interdependencies/criticality of the area:

- The close connection of physical and cyber threats on critical infrastructures requires particular attention; both regarding to emergence, as well as to the preparation against such threats (see sub-section 2.2.1).

Policy links:

- Internal Security - COM(2009) 273 final CBRN Action Plan
- Civil Protection - Decision 1313/2013 EU Civil Protection Mechanism
- Environment - Decision 1386/2013 Environment Action Programme
- Environment - Directive 2012/18/EU (Seveso III Directive)
- Consumer Health - Decision 1082/2013 Serious cross-border threats to health
- Energy - Regulation 347/2013 Guidelines for trans-European Energy Infrastructure

- Transport - Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU
- Enterprise & Industry The Security Industry Policy (COM (2012) 417)
- The European Programme for Critical Infrastructure Protection (EPCIP)
- Towards a stronger European disaster response: the role of civil protection and humanitarian assistance, COM(2010)600
- European Union Maritime Security Strategy
- Council Decision of 24 June 2014 on the arrangements for the implementation by the Union of the solidarity clause (2014/415/EU)
- Commission Staff Working Document on Transport Security SWD(2012)143 final of 31.5.2012
- Commission Communication of 8 April 2014 on opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner

2.1.2. Fight against crime and terrorism

The ambition in this area is to provide research results and knowledge necessary to avoid an incident and to mitigate its potential consequences, including new technologies and innovative capabilities for fighting and preventing crime (including cyber-crime), illegal trafficking, and terrorism (including cyber-terrorism), and for understanding and tackling terrorist ideas and beliefs.

In this area, no specific legacy actions from the Work Programme 2014-2015 require a follow up. The scope of the area could remain as is and described in a more general way. A few additional domains were highlighted during discussions with stakeholders that could be also usefully covered in the next work-programme:

- Preventing of radicalisation and recruitment to terrorism and violent extremism.
- Enhanced law enforcement/public safety information exchange model to ensure that the competent authorities can simply and lawfully access crime-related information from numerous sources.
- A holistic approach on the exchange of international crime and terrorism related data should be envisaged and designed.
- Citizen's reporting on crime.
- New emerging risks – designing for security, potential dangers of technologies considered from the outset; addressing crime prevention within the early stages of the product development process; assessment of the costs and benefits, internet frauds.
- User-communities or groups of stakeholders concerned with specific issues should be encouraged to organize with a view to coordinating further research work and expressing requirements.
- Forensics – full extensive exploitation of all type of traces; introducing new innovative analysis technologies; make forensic quicker, less costly, more precise.
- Detection: expanding detection capabilities.

Interdependencies/criticality of the area:

- Fight against crime and terrorism tightly relates with privacy and ethics (see sub-section 2.2.3).

Policy links:

- Political Guidelines for the next European Commission "An Area of Justice and Fundamental Rights Based on Mutual Trust"
- EU Internal Security Strategy in Action (COM(2010) 673 final);
- An open and secure Europe: making it happen (COM(2014) 154 final)
- EU Action Plan on Enhancing the Security of Explosives (Council (2008)8311/08);
- Prevention, preparedness and response to terrorist attacks, COM(2004) 698
- Revised Strategy on Terrorist Financing (2008)
- The European Union Counter-Terrorism Strategy (2005) & The EU Action Plan on combating terrorism (revised as of 2007)
- The EU Strategy towards the Eradication of Trafficking in Human Beings 2012–2016, COM(2012) 286
- Customs Risk Management and Security of the Supply Chain, COM(2012) 793
- EU Strategy and Action Plan for Customs Risk Management, COM(2014) 527
- EU Charter of Fundamental Rights
- European Convention on Human Rights
- Commission Staff Working Document on Transport Security SWD(2012)143 final of 31.5.2012

2.1.3. Border and external security

This area targets the development of the novel technologies and processes required to:

Border Security:

- Enhance systems, equipment, tools, procedures, and methods supporting the border control authorities to ensure the security of the EU external borders, covering legal and irregular migration, whilst at the same time facilitating the legitimate flow of people and of goods.

External Security:

- Support the Union's external security policies in its civilian tasks, ranging from civil protection to humanitarian relief, border management or peace-keeping and post-crisis stabilisation, including conflict prevention, peace-building and mediation.

Three Coordination and Support Actions (CSA) are being launched in 2014-2015, which may be worth continuing with a next logical phase: in the area of technological support for civilian humanitarian mission (follow-up to BES-10), in the area of Information management, systems and infrastructure for civilian EU External Actions (BES-11), and in the area of civilian conflict prevention and peace building capabilities of the EU (BES-12).

Further to the above-listed “legacy” actions from the Work Programme 2014-2015, the scope of the area could remain as is and described in a more general way. A few additional domains were highlighted during discussions with stakeholders that could be also usefully covered in the next work-programme:

Border Security:

- The development, pre-commercial procurement and innovative use of low-cost technologies, possibly dual-use assets, to enhance maritime surveillance involving EU agencies, such as Frontex and European Maritime Safety Agency, and the Member States;

- Closing the gap between what is currently available and what is technically feasible and financially affordable, either in projects where industry takes the lead in developing, in close consultation with the Member States and Frontex, or in pre-commercial procurement;
- Permitting the effective authentication of electronic travel documents, both from our own citizens as those of third countries;
- The use of Frontex and the Joint Research Centre of the European Commission in analysing and disseminating the results of FP7 and Horizon 2020 projects among the Member States' border control authorities;

External Security:

- The increasing exposure of humanitarian actors to zones of instability and conflict calls for further research on the development of innovative means to ensure the security of humanitarian actors and the efficient delivery of humanitarian aid.

Interdependencies/criticality of the area:

- Border security closely relates with privacy and ethics (see sub-section 2.2.3).

Policy links:

- Political Guidelines for the next European Commission "Towards a New Policy on Migration"
- Regulation (EC) n°725/2004 on enhancing ship & port facility security
- EU Internal Security Strategy in Action (COM(2010) 673 final)
- The European Border Surveillance System (EUROSUR)
- The SMART Borders initiative
- The European Union Maritime Security strategy
- Customs Risk Management and Security of the Supply Chain, COM(2012) 793
- EU Strategy and Action Plan for Customs Risk Management, COM(2014) 527
- European Union Maritime Security Strategy
- EU Charter of Fundamental Rights
- Commission Staff Working Document on Transport Security SWD(2012)143 final of 31.5.2012

2.1.4. Cybersecurity for all

One top challenge of the coming years is to translate cyber security concepts into workable and available services for citizens and small enterprise so that levels of cybersecurity can gradually increase to enhance the trust of online users. This implies addressing not only issues of resource-efficiency of solutions for users, but also taking into account user-specific factors, such as accountability, liability transparency, usability, cyber-economics and behavioural ICT. Workable solutions will need to provide a high degree of automation for aspects beyond the competences of non-specialist users, while making sure that users retain an adequate degree of awareness, control as well as privacy over their online activities.

Apart from focussing on the needs of citizen users, particular focus will have to be placed on SMEs to reduce their burden for implementing cyber protection (e.g. protect their IPR and their supply chains against security breaches, improve security of transactions, avoid internal and external fraud and data theft) and help them to comply with the law.

In addition, support for SMEs in the field of cybersecurity should be envisaged as well by using the opportunities offered by the single market to increase the demand for their solutions. This would for instance look into self-declaration and cheaper/faster mechanisms than standardisation/certification. Action here would also facilitate the emergence of SMEs through incentivising the development of secure solutions for high-added value niche markets.

Policy links:

- Political Guidelines for the next European Commission "A Connected Digital Single Market"
- Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace
- Competitiveness and innovation of European enterprises and support policies for Small and Medium Enterprises (SMEs).
- International collaboration in the field of cybersecurity and implementation of the EU Cybersecurity Strategy
- Protection of fundamental rights and data protection regulation.
- EU Internal Security Strategy
- European Cyber Security Centre (EC3)
- Security in electronic and mobile payments and in cross-border internal market services.
- Protection of vulnerable consumers, development of safe on-line trade environments, enforcement cooperation.

2.2. Novelty through adaptation to evolving threats and needs

Compared with the year 2013 when the first work programme was drafted, the context for security research has changed in one aspect in particular: that of the emergence of threats to critical infrastructure that combine the risk of cyber-attacks with that of physical attack, and to which the response also needs to combine cyber and physical security solutions.

Ethical and fundamental rights concerns related to security research are increasing, and they intermingle with further privacy issues arising from the development of the large data repository associated with many security solutions, raising the need for comprehensive research effort in this area.

Also, the Security Advisory Group advised that, in light of staff and budget cuts in national administration, the risk is high to see the users of security solutions investing even less than in the past into defining their requirements for future technologies and innovation. Pan-European networks of users would need more support to perform this task (together with European agencies active in their respective areas), as well as to share their capabilities (e.g. their testing sites and specialized laboratories) in a more coordinated way across Europe.

Such contextual changes advocate for concentrating activities in the following ways:

2.2.1. Solutions addressing targeted, combined cyber and physical threats against European infrastructure; and enterprises

It has been a trend in the last years that advanced persistent threats and related forms of botnets, malware etc. follow increasingly elaborated strategies to attack specific targets, while often incurring significant economic damage without being detected in time. More specifically, cybercrime is now the largest common factor across all critical services and infrastructures as a

result of the increasing pervasiveness of ICT and the growing interdependencies between physical and cyber infrastructure. While the threats are increasing, protecting critical infrastructure from cyber-attacks became the largest current challenge of the Critical Infrastructures domain.

Defences need to be built up to counter the increasing vulnerabilities of these victims, be they public organisations, law enforcement agencies, critical infrastructure providers or large enterprises. In most attack scenarios, it is no longer sufficient to rely on single lines of defences as these – once breached – enables attackers to gain access to all parts of an organisation. To counter such targeted attacks, it must be a priority to increase the resilience of organisations by a number of measures, such as situational awareness for early responses, intrusion-tolerant systems to mitigate the damage of breaches and also give support to counter specific emerging online threats.

Policy links:

- Political Guidelines for the next European Commission "A Connected Digital Single Market"
- Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace
- The protection of fundamental rights and data protection regulation.
- The fight against cybercrime in relation to the EU Internal Security Strategy) and link to Europol, as well as the recently-adopted Directive 2013/40/EU on attacks against information systems and the recently-transposed Directive 2011/92/EU on combating the sexual exploitation of children online and child pornography.
- Security in electronic and mobile payments and in cross-border internal market services.
- The industrial policy aspects, in particular investment in R&I and standardisation as well as for R&I in the area of critical infrastructures and security.
- The Security Industry Policy (COM (2012) 417)
- Enforcement of on-line consumer rights

2.2.2. Privacy

With the increased number of security and digital applications, the volume of personal data being collected, processed, stored, and shared has dramatically increased.

In our digital society, the collection, processing and sharing of personal information, often referred to as the "currency of the digital era", has contributed significantly to the emergence, commercial success and rapid evolution of innovative business models. In the near future, the volume and rate of collecting and processing of personal information is expected to grow further with new paradigms such as Big Data and the "Internet of Things" (IoT) promising further opportunities in data centric innovation. Meanwhile, new and advanced methods for tracking online behaviours also present new threats to the fundamental value of privacy as well as to the protection of consumers against unfair commercial practices.

In this context, public opinion expresses more and more the need to protect such data, to drastically improve the transparency of how this data is being handled, to reduce intrusions into the privacy of an individual to a minimum and to protect consumer rights.

Going beyond protecting personal information from unlawful disclosures, research and innovation actions are required to successfully address all the requirements already present in the

text of the EU Data Protection Directive 95/46/EC as well as new challenges stemming from the novelties discussed under the draft General Data Protection Regulation currently in the law-making process. The former include, for instance, the general data protection principles such as the fair and lawful collection and processing of data, purpose limitation, accuracy, retention limitation, etc. The General Data Protection Regulation-specific novelties include, for instance, the right to data portability, the right to be forgotten, data protection impact assessments and the various implementations of the principle of accountability.

Even though research and innovation into the technological aspects surrounding privacy are fundamental, equally challenging issues arise from the way technology, business processes and human behaviour intersect. Trust of citizens, perception, beliefs, emotions and values as well as behaviours should be further studied.

Policy links:

- Political Guidelines for the next European Commission "An Area of Justice and Fundamental Rights Based on Mutual Trust"
- The Charter of Fundamental Rights of the European Union (in particular Article 8)
- The Data Protection Directive 95/46/EC
- The ePrivacy Directive 2002/58/EC
- The Data Protection Regulation (EC) No 45/2001 relating to processing by Community institution and bodies and on the free movement of such data.
- The Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
- Joint Communication Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final
- The Security Industrial Policy (COM (2012) 417)

2.2.3. Ethics

The demand for novel security technologies has increased over the last years. Anti-terror legislation has become a main driver for the development and deployment of such security technologies. This is leading to the emergence of new research domains related to the ethical and societal dimension of security, including:

- Better understanding the links between culture, risk perception and disaster management, particularly in a context of increased migration within the Union posing greater challenges to authorities, including first responders.
- Enhancing cooperation between law enforcement agencies and citizens.
- Better understanding the role of social media.
- The processes that lead to organised crime, violent radicalisation and insider threats.
- Human factors in border control and other security areas.
- Balance between security and privacy in the digital World.

Society and security aspects should be further exploited. Trust of citizens, perception, beliefs, emotions and values as well as behaviours should be further studied. One issue which was not that often covered by our projects is security and immigration. Additional focus might be put on research addressing questions how Privacy by design and by default or data protection by design

and default could be embedded in the innovation models or systems from economical point of view – whether this will be expensive and if so how to make it more economical.

Policy links:

- Political Guidelines for the next European Commission "An Area of Justice and Fundamental Rights Based on Mutual Trust"
- The Charter of Fundamental Rights of the European Union (in particular Article 8)
- The Data Protection Directive 95/46/EC
- The Data Protection Regulation (EC) No 45/2001 relating to processing by Community institution and bodies and on the free movement of such data.
- The Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
- The Security Industrial Policy

2.2.4. Horizontal actions

Pan-European networking is required with a view to achieving a number of coordination objectives:

Overarching target: the establishment of organised, pan-European end-user communities concerned with innovation in the field of security

User-communities of security research in Europe (first responders, police forces, civil protection units, financial fraud, border guards, etc.) are rarely organized in a pan-European manner, and even when they are, have little resources to work at two issues essential to the continuation of European security research programmes:

- firstly, defining their needs in terms of innovation through interaction with ongoing European and national research projects and providers;
- secondly, ensuring a proper transfer (and implementation) of research outputs and pan-European innovative security solutions to actual operational "users".

Overarching target: pan-European networks of demonstration and testing sites for security research

Building up on the experience gained by demonstration projects in areas where they exist (e.g. EDEN on CBRN-E detection and DRIVER on crisis management), or starting from scratch in similar areas (e.g. maritime security), the establishment of pan-European networks capable to host the demonstration or the testing of novel security solutions would fulfil an obvious gap that exist today at European level.

Overarching target: developing international cooperation in security research

International cooperation is possible through the Challenge. Existing or future implementing arrangements of science and technology agreements (e.g. with the US Department of Homeland Security S&T Directorate) are encouraging cooperation further in some more specific areas referred to in such arrangements (e.g. innovation for first responders; global maritime security).

Given the sensitivity of some research domains cooperation is recommended with countries where security research is guided by principles that share a lot of commonalities with Horizon 2020 principles, in particular as regards privacy and ethics (“Think-alike countries”).

Cooperation is encouraged when it can be motivated in terms of European interest – be it in terms of access to technologies, facilitation to export, or else (e.g. with non-European Mediterranean countries when cooperation facilitates the deployment of innovative security solutions), as appropriate.

Pan-European networks could focus on drafting the requirements for international cooperation in security research with some non-European countries when activities in such countries are broad enough to motivate the establishment of across-the-Challenge cooperative research strategies (e.g. some Horizon 2020 Associated countries, the US, Canada, Australia, etc.)

Policy links:

- The Security Industrial Policy

3. Translation into calls 2016-2017

It would be premature to give definite indications on the exact number and titles of the calls for the Secure Societies Work Programme 2016-2017. Consultations on the future orientation of the Secure Societies challenge have however clearly indicated that a certain level of continuity should be maintained throughout the structure of the work programmes from 2014 to 2017:

- The areas covered by Disaster Resilience, Fight against crime and terrorism, and Border and external security would thus continue to be covered in the 2016-2017 work-programme, with slight modifications and the reduction of the number of topics;
- The Focus Area “Digital Security” would evolve as described in the appendix below;
- Four Calls could be added, resulting from the needs identified under the “adaptation to evolving threats and needs” section above.

This would lead to the following eight calls:

1. Continuity	2. Novelty through adaptation to evolving threats and needs
1.1. Disaster Resilience	2.1. Combined cyber and physical security of European infrastructure and enterprises
1.2. Fight against crime and terrorism	2.2. Privacy
1.3. Border and external security	2.3. Ethics
1.4 Digital Security	2.4. Horizontal actions (networking)

Focus Area Digital Security

Given the growing challenges to the maintenance of online security, it is considered that Digital Security would be a pertinent focus area for the Strategic Programme 2016-2017. Research and innovation in the cybersecurity would benefit European users and business that increasingly base their economic activities and social life in the digital world. Supporting innovative approaches to ensure digital security will limit the damages of online attacks, service disruptions and data

breaches and subsequently maintain the trust of online actors. As Europe's society and economy is increasingly based on digital services (in a diversity of fields, such as transport, energy, finance etc.), any negative impact on the security of such service will have negative consequences on the functioning of society, economic growth and the technological innovation potential of Europe.

ICT-driven transformations across all the sectors mentioned above bring vulnerabilities to critical infrastructures and services – both public and private. For example, in the energy sector, in 2012, the computer network of Saudi Arabia's national oil and gas firm (Aramco) was struck by a self-replicating virus that infected 30,000 PCs. In transport, a drug gang last year hacked into Antwerp seaport systems to break into the systems of shipping companies. In health, Community Health Systems, a major US hospital group, just recently said it was the victim of a cyber-attack resulting in the theft of 4.5 million people's personal data. Therefore, as digital security and privacy are explicitly mentioned in the Specific Programme texts of Societal Challenges 1 'Health, demographic change and wellbeing', 3 'Secure, clean and efficient energy', 4 'Smart, green and integrated transport' and 6 'Inclusive, innovative, and reflective societies', more efforts are necessary here to create a comprehensive approach on security and privacy in the Societal Challenges.

Societal Challenge 1 'Health, demographic change and wellbeing' and 'Leadership in Enabling and Industrial Technologies - Information and communications technology' are expected to contribute to this focus area.

Further research and innovation in societal challenges and leadership in enabling and industrial technologies is required to continue effective mitigation efforts for emerging threats and advance persistent threats that focus resources on targeted attacks. Research and innovation activities are also necessary to create and test new frameworks for real-time situational threat awareness and immediate response against attacks while providing new models for risk mitigation by innovative resilient intrusion/compromise tolerant systems.

In addition, the increased interdependence between infrastructures, for example in smart cities environments, amplifies vulnerabilities. Analysing and, eventually, securing these complex systems requires bringing together actors from all the different sectors and across the EU.

Finally, Cybersecurity has been regularly stated in many EU policies pertaining to infrastructures (i.e. public sector, smart grids, intelligent transport systems, banking and finance, manufacturing), including the EU cybersecurity strategy itself.

This focus area would be the opportunity to address the scientific and industrial challenge that this concretely represents by breaking through sectorial approaches and bringing economies of scale by providing coherent solutions that will work both inter and intra sectors.