Horizon 2020 - Societal Challenge 7:

Secure societies – protecting freedom and security of Europe and its citizens.

Report of the Protection and Security Advisory Group (PASAG)

July 2016

In accordance with the mandate of the Protection and Security Advisory Group (PASAG), this report aims to identify the scientific, technological and innovation priorities for the Horizon 2020 Societal Challenge 7: Secure societies – protecting freedom and security of Europe and its citizens. The report is based on the results of the PASAG discussions and comments provided by its members.

Foreword by Alberto de Benedictis, Chair of the PASAG

The recent (and past) grave incidents in Europe clearly point to two enablers of terrorist and criminal capability: unfettered access to technological innovation and a weak EU-wide security framework. In other words, technological innovation has made the task easier for those who want to perpetrate harm and harder for those who defend against them.

Much work is already underway at European level to strengthen the EU-wide security framework. We are seeing greater co-operation and data exchanges across national boundaries. We must also ensure that practitioners[1] have access to the technological enablers for the capabilities they need. The Secure Societies work is producing new and improved technologies and security solutions to strengthen practitioner capabilities and the competitiveness of the European security industry. The Horizon 2020 Secure Societies programme represents by far the most significant source of funding in Europe for the development of security technology and innovation. It is imperative therefore that forthcoming funding rounds take heed of the lessons learned to date.

With this in mind, PASAG considers the following general themes should be taken into account in drawing-up future work programmes:

First, build on the steps already taken to achieve greater involvement of practitioners in the research and innovation actions. This is key to helping 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

[1] Throughout this paper, "practitioners" is interpreted widely to include security service providers, law enforcement agencies and end-users, both public and private.

State (MS) institutions. EU support to knowledge networks adds value by knitting together EU-wide communities of interest.

Second, encourage and support an effective and functioning network of security practitioners and first responders, not just to disseminate best practices and the outcomes of innovation and research actions, but to enable a more effective, real-time institutional response to crises.

Third, ensure that future programmes can adapt to changing circumstances and, where necessary, provide for new actions. Crime, terrorism and natural catastrophes do not conform to a predictable view of events and consequent policy responses. Technology is evolving rapidly. Within its longer term strategic vision, the Secure Societies programme needs to be sufficiently flexible to react, for example with additional calls, to new developments when actions need to be taken in response. Where Secure Societies provides the underpinning for Europe's security capability development, it must be quick to adjust to circumstances and continue to stay relevant.

Fourth, we need to continue to reduce the barriers to cross-border co-operation – of Member States, of industry and of practitioners – and to promote a greater take-up by practitioners of the outputs of Horizon 2020. Some progress has been made: special programme modalities now provide that research output will be made available at Fair, Reasonable and Non-discriminatory terms. More is needed to bring technologies much closer to market exploitation and enable a greater and faster adoption by practitioners, particularly by ensuring that outcomes of research programmes are disseminated more broadly and that the technological developments that are produced can find a path to market in a useful time-frame. Consideration should be given to utilising EU funds (one example is the Internal Security Fund) to incentivise member States and practitioners to exploit the outputs of Horizon 2020, consistently with EU rules. More European standards (beyond the current limited scope of alarm systems and airport scanners) are needed to help ensure that security solutions can be applied across borders without the need for specific adaptations to local requirements.

Fifth, we need to expand collaboration between the public and private sectors in the field of civil security. The public private partnership (PPP) instruments, notably the new PPP on cybersecurity, are creating interest in new governance models with varied stakeholders. This should help develop security capabilities that would otherwise be unaffordable or impractical. It also encourages the development of market-oriented solutions, because a healthy and innovative security industry is critical to ensuring that the EU can continue to meet its evolving threat challenges. Other models 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. Demonstration pilots on how these might work and the incentives that business would need to become engaged and committed, could usefully be launched at the European level.

Sixth, investment in security capabilities should not be addressed exclusively within the Secure Societies programme. 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 through Horizon 2020 focus areas would ensure that security implications are properly considered and complement the initiatives launched under Secure Societies. PASAG will encourage relevant Advisory Groups within Horizon 2020 to engage on the potential security implications within the programme areas in their remit.

These considerations have framed the work of PASAG to date. In this first report, we set out our "Visions" for 2030 in 5 areas and our advice to the European Commission for the development of the next Work Programme (2018-20) of the Secure Societies theme in Horizon 2020. It builds on the work undertaken by our predecessor the Secure Societies Advisory group[2].

Introduction

Under the Specific Programme implementing Horizon 2020, Societal Challenge 7 "Secure societies – protecting freedom and security of Europe and its citizens"

[2] Earlier reports from SSAG can be found at http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3010

concerns the research and innovation activities needed to protect our citizens, society and economy as well as our infrastructure and services, our prosperity, political stability and wellbeing.

The primary aims of the Secure Societies Challenge are:

- to enhance the resilience of our society against natural and man-made disasters, ranging from the development of new crisis management tools to communication interoperability, and to develop novel solutions for the protection of critical infrastructure;
- to fight crime and terrorism ranging from new forensic tools to protection against explosives;
- to improve border security, ranging from maritime border protection to supply chain security and to support the Union's external security policies including conflict prevention and peace-building;
- and to provide enhanced cyber-security, ranging from secure information sharing to new assurance models[3].

The Protection and Security Advisory Group (previously called Horizon 2020 Secure Societies Advisory Group) was renewed in 2015. Its members are listed in Annex A. Its mandate from the European Commission is to "provide consistent and consolidated advice to the Commission services during the preparation of the Horizon 2020 work programme." The Commission have asked that "advice should be provided on relevant objectives and scientific, technological and innovation priorities by way of opinions, recommendations or reports."

Priority Security Areas

For the purposes of this report, the PASAG has identified five key areas that represent priority domains for the forthcoming funding periods:

i) Borders and External security
ii) Fighting Crime and Counter-terrorism
iii) Secure and Resilient Societies
iv) Cybersecurity and Privacy Technologies
v) Competitive European Security Industry

For each area we set out a "vision" for 2030, to ensure that what gets funded today represents stepping stones along a technology roadmap that has the ultimate objective of delivering tomorrow's vision. We believe that by providing a longer term view we can track more effectively the timeline necessary to produce innovation and technology leadership in security solutions. Our emphasis on closer and stronger engagement with practitioners and user

[3] https://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens

communities is motivated by the need to extend the solution horizon beyond the response to the immediate threat or current crisis. Assisting both industry and users to plan for the longer-term is an incentive that we expect to be built into the next cycle of funding programmes.

We then describe: the main challenges; the Research, Development and Innovation (RDI) milestones; and where appropriate, the new markets that may develop and the emergent technologies that may disrupt or induce paradigm changes.

i) Borders and External security

Vision for 2030

- EU citizens of good standing 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

- Integrated border management through a common interface (air, land or sea; people or cargo; transportation modes.)
- Developing a comprehensive border technology roadmap
- Establishment of an 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

- Effective co-operation and joint activities with relevant national and European bodies and Agencies (e.g. EDA, Europol, Frontex, EMSA, EEAS, customs) including managing irregular migration while facilitating legitimate travel[4], with relevant third countries, and co-operation activities at regional level (using Structural Funds);

[4] As already advised by SSAG, section 5.2 of its report of December 2015

- Co-operation frameworks between industry and practitioners to implement technology investment road maps, and provide essential capabilities;
- Systems, equipment, tools, processes and methods for rapid identification for both control and surveillance issues, exploring the potential of EUROSUR and CISE[5] and promoting new technology for border checks;
- a comprehensive approach 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;
- Large scale pilots in cooperation with industry and end-users, meeting practitioners' requirements, and evaluating and implementing state-of-the-art capabilities.

New Markets

- Advanced security products with access to an open EU and export market;
- IT architectures, 'big data' solutions and man-machine interfaces, integrating legacy and new systems across multiple countries;
- Private sector ownership of assets and service provision of border management capabilities;

Emerging/disruptive technologies

- 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;

ii) Fighting crime and counter-terrorism

Vision for 2030

- EU citizens and residents in good standing are able to live and operate in peace and freedom, with no significant threats or risks to their lives or property, including in the digital environment.
- As crime and terrorism continue to evolve from the physical to the virtual world, from localised to international, and from socially-connected groups to virtually-connected anonymous networks, there will be increased success in predicting, monitoring, recognising, and preventing them.

[5] CISE – Common Information Sharing Environment – to enhance information sharing between maritime surveillance authorities

- This will be achieved through faster or real-time responses, with improved exploitation of advanced digital tools such as metadata and social engineering, including community of interest groups created to protect their members. Criminal behaviour and networks will be detected, identified and inhibited earlier with capabilities being thwarted before criminal networks and groups can achieve scale.
- Law enforcement will focus on meeting new technological challenges including in encryption and privacy protection. Law enforcement agencies will have the latest technology to detect, investigate and prevent criminal activity. Enhanced techniques for tracking criminal behaviour within the virtual world will increase the risks for criminals.
- Technological advances will make evidence more robust thus enabling reactive, efficient and fair justice systems.

Main Challenges

- Nature of the threats to EU citizens and organisations is evolving rapidly and becoming more international;
- Radicalisation of groups or individuals, also in response to events outside the EU;
- Shortage of technical skills in security and law enforcement agencies, particularly skills in preventing, detecting and tackling cyber-crime;
- Differences in national laws and approaches make it more difficult to implement best practices and research outcomes, which have to be adapted to local conditions and requirements;
- Increasing use of open source technology by public services may hinder innovation by industry which prefers commercially proprietary technology;
- Human factors need to be studied scientifically in the light of societal changes and taken into account in all aspects of research to support counter-terrorism and fighting crime;
- New technologies are facilitating financial and economic crime (e.g. crypto-currencies, IPR theft);
- Technology to protect citizens may hinder law enforcement access to evidence - the challenge is to find the right balance;

R&D&I milestones

- Analysis of digital evidence is as automated as possible, even at local level;
- Big data analytics, based on open source technology, enables early detection of criminal activity;
- European standards support exchange of information, intelligence, data and evidence between law enforcement services and agencies;
- New technologies support reduction in the use of force by enforcement agencies (for example, immobilising vehicles electronically);

New Markets

- Private security services for both public and private domains;
- Cybersecurity and cyber assurance;

Emerging/disruptive technologies

- Quantum computing (e.g. for decryption);
- Artificial Intelligence and man/machine interface;
- Use of nanotechnology in investigation techniques;
- Autonomous systems (e.g. robots, UAVs) for use in enforcement and detection;
- Special purpose malware;

iii) Secure and Resilient Societies

Vision for 2030

- European society, government and commerce, and the services they depend on will be 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 is co-ordination and co-operation on security and resilience at all levels of society. Disaster relief agencies and first responders are well-equipped and effective and co-operate well across national borders.
- Citizens and companies 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 are 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 is available.
- Global co-operation and harmonisation of regulations mean that supply chains are trustworthy and trade is thriving.

Main challenges

European society is a complex network of individuals, organisations, and communities. These elements are dependent on each other, on allies and trading partners, on shared infrastructures, and on technology. The values, functions, and well-being of society and its members are at risk from a variety of natural, accidental, political, economic and malicious threats. The goal of the Secure and

Resilient Societies programme is to limit exposure to such risks, mitigate their impact and enable rapid recovery from their effects. This includes addressing questions of national and transnational vulnerabilities, resilience and capabilities related to prevention, preparedness, response and recovery. The programme should target identified high-priority threats, protections and counter-measures and also develop, validate and pilot generally-applicable models and principles.

We have distinguished 3 main sub-themes:

a) Disaster resilience: following on from the DRS theme of previous H2020 rounds;
b) Secure and resilient organisations and infrastructure: following on from the CIP theme of previous H2020 rounds, but going beyond organisations providing critical infrastructure. We propose a focus on multi-disciplinary research taking a holistic view of organisations and their environment as interacting people, processes, technology and physical infrastructure; and
c) Societal issues: such as research into the appropriate balance between individual freedom/privacy and collective security, public attitudes to security, motivating and empowering citizens, and new social and governmental mechanisms.

a) Disaster Resilience

- Improve risk assessment, mitigation and early warning inside and outside the EU;
- Improve interconnection and interoperability of systems, equipment and procedures for disaster and crisis management and support standardisation of such equipment and systems,;
- Provide enhanced situational awareness for actors and management levels, including decision-makers, back-office experts, and first responders;
- Improve education and preparedness for disasters across the EU, including individuals, first responders and policy makers;
- Improve coordination of activities at EU and international level, with better cooperation and cross-fertilisation between different sectors, including synergies with the military domain;
- Improve EU support to international disaster management.

b) Secure and resilient organisations and infrastructure

- Ensuring networked and automated critical infrastructures are secure and resilient to malicious, natural and accidental disruption;
- Providing trustworthy and resilient Europe-wide infrastructure that is accessible to all and supports the full range of governance, economic and societal activities and goals;

- Lack of a practical theory and engineering discipline supporting design and operation of complex, secure and resilient organisations and societies;

c) *Societal issues*

- Achieving societal consensus on the balance between collective security and individual privacy/freedom, while including and empowering all sections of society.
- Establishing trust in the complex dependencies on public and private service providers and supply chains.
- Blurred responsibilities for societal security - private-public domains, local, regional, national, EU levels of authority.
- To be resilient, a community needs resilient individuals. We need leadership to enable individuals, communities, and organisations/administrations to build resilience at every societal level.
- Prevention of radicalisation of EU citizens and how to de-radicalise those affected.

R&D&I milestones

a) Disaster Resilience

By 2020 and updated thereafter*:*

- Development of guidelines, methods and tools to highlight best practice and strengthen cross-border interoperability of first responders.
- Integration of existing systems and tools for operational use by various actors.

b) Secure and resilient organisations and infrastructure

By 2020 and updated thereafter*:*

- Development of guidelines for designing, constructing and managing secure and resilient organisations and social systems, and for the use of adaptive security and resilience techniques in such systems.
- Large scale pilots in industry and public sector exemplifying the vision of secure and resilient organisations and using the above methods, tools and institutions.

c) Societal issues

By 2020 and updated thereafter:

- Identification of the key features of the trusted institutions and services under-pinning secure and resilient societies;
- Inter-disciplinary research on ways to motivate and empower communities to contribute to security and resilience, and means of

achieving societal consensus *beyond 2020:* trials involving active citizen participation;

- Guidelines for the design of institutions for governance of security and resilience aspects of societies;
- Increased knowledge and technical solutions for detection of societal vulnerabilities;

New markets

- Innovative commercial services/institutions for a range of secure and resilient organisations and social systems.

Emerging/disruptive technologies:

- Decentralised institutions, e.g. based on blockchain[6] technology
- Autonomous, intelligent systems (e.g. robots, UAVs, sensors) for use in detection and response
- Social media/networks, application of gaming principles to non-game contexts.

iv) Cybersecurity and Privacy Technologies

Vision for 2030

- Cybersecurity and Privacy technologies will have developed so they are mutually supportive and complementary enablers of the European digital economy, ensuring a secure and trusted networked environment for governments, businesses and individuals.
- Cybersecurity and Privacy are at the very centre of how network, information and communication technologies (ICT) are designed, managed and controlled, encouraging exploitation and deployment of these capabilities in Europe and internationally.
- New cybersecurity and privacy systems and protocols will position the EU as a world leader in building a safer and more secure digital economy.
- Citizens and customers will benefit from user-friendly and accessible security 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.
- Specialized systems in sensitive areas such as health and finance will be major spheres of innovation aiding public confidence in, and growth of, diverse market sectors.

[6] Blockchain identifies a distributed ledger technology that enables peer-to-peer secure transactions without third party involvement or verification. Once a transaction is executed and confirmed a record is made and permanently retained. The first broad usage of blockchain was initiated through Bitcoin transactions but offers great scope for far wider application.

Main challenges:

- Cyber-protection of digital and physical resources connected to digital networks from disruption (such as intentional malicious or criminal cyber-attacks, unintentional malfunction, etc.) that can damage and impact society, economy, freedom, privacy and security.
- 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;

R&D&I milestones to build an EU Digital Research and Innovation ecosystem, aligned with the Digital Single Market (DSM)

We need specific investments in EU core technologies and new assurance models. Processes should be re-designed so that Cybersecurity and Privacy are at the heart of how network, information and communication technologies are designed, managed and controlled, while maintaining a balance between individual privacy/freedom and judicial investigation and enforcement. This will encourage the exploitation and deployment of these capabilities in Europe and internationally. Hitherto, security and privacy requirements have been insufficiently 'built into' the design, manufacture & deployment of ICT technologies with resultant vulnerabilities. European values and fundamental rights must be considered as a competitive advantage and a business driver.

Specific R&D&I milestones:

- Promoting investments in EU Cyber-security and privacy "core-related" technologies (e.g. encryption, Identity Access Management (IAM) capabilities, hardware security) to secure the cyber environment. Plus other technologies e.g. nanotechnologies, advanced manufacturing which might offer a competitive advantage for EU. End users, Member States and Industry to decide criteria for such investments.

- Dynamic certification for Cybersecurity assurance, based on European (or, as appropriate, ISO) standards without fragmenting the global market. Such a model of Cybersecurity and privacy safeguards will ensure EU products and services fully comply with end user security and privacy requirements while maintaining the balance between individual privacy/freedom and judicial investigation and enforcement. Such a model can be a potential worldwide standard. It must consider EU and foreign components, products and services in order to grow the level of trust in EU public/private networks and systems worldwide. The model might also consider the "Privacy Shield" (US-EU) and any other privacy related agreement between EU and other trading partners.

- Pilot Cybersecurity and Privacy Assurance Model specifically with SMEs to demonstrate efficient and effective model for dynamic certification of products and services along lifecycles.

- Develop an effective "EU Cybersecurity and privacy Testbed", available for researchers, entrepreneurs, SMEs to foster:

  - Interoperability between EU products and services
  - Simulation and training (for eSkills environment)
  - Shared data: availability of real exchange of data and intelligence while developing products
  - interconnected research and innovation at EU level and market intelligence as well as facilitating fast track innovation

- Verification of combinations of security measures, tools and products (noteworthy is the explosion in the number of devices).

- Develop large scale security risk modelling tools to help, for example, understand the financial impact on our economies and society.

- Pilot projects on IAM, crypto and other core technologies.

New markets:

- Privacy Enhancing Technology (PET)

- Hardware embedded security

- Assurance

- Internet of Things (IoT/Internet of Everything (IoE).

In general, All domains and All things which have connection (both hardware and software) such as automotive, health, production, critical infrastructure as well as things like food chains, medical devices and drugs, constructions like bridges, tunnels etc.

Emerging/disruptive technologies:

- Electrical ubiquity (as an example)

- Home-based (cloud) enterprises

- Quantum and post-quantum cryptography

v) A competitive European security industry

Vision for 2030

- The European security industry is 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 has been achieved through strategies to connect effectively supply and demand sides of the markets. The shared knowledge base of the security ecosystem is enhanced through new networks linking innovation paths of mutual interest and making available non sensitive information on a rapid basis. This is generating significant wealth including through the combination of small agile companies with more established businesses and multi-national corporations
- To deploy innovative technologies and solutions 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. This is underpinned by recognition and trust, achieved through high levels of professionalism, based on education, skills and training.

Main challenges

Supporting a digitally connected Global Market:

- Development of European standards, defined jointly by industry and operators/users, to underpin this market.
- The reluctance of Member States to relinquish national controls and requirements on standards for security and security products can damage competition.
- The fragmentation of the European market hinders the emergence of pan-European operators.
- Effective deployment of innovative technologies needs a true single market for security and security products (e.g. crisis management guidance/toolkits, CBRN (chemicals, biological, radiological, nuclear) explosives, biometric technological solutions, security in healthcare facilities.
- Funding, especially for SMEs, for exploitation of innovative technologies to encourage commercialisation of research outputs.

Deployment of innovative technologies:

- The current fragmented security market will hinder the creation of a coherent single European security market and will make it more difficult to agree industry-led common standards.

Skills & Education

- We need professionals who can work across sectors (to avoid silo mentality which discourages innovation) and have a better understanding of IPR.
- New emerging markets will require new professions where a targeted/ personalised and cross sectoral approach is needed.

R&D&I milestones

- Create networks and test beds (PPPs, Networks of excellence) for e.g. cybersecurity to ensure a coherent approach with EU DSM;
- Establish facilitate EU-based "clusters" of industry and operators/users to define and develop: technological solutions to improve supply chain security; propose protocols for data exchange and protocols for interface with space technology (e.g. Galileo);
- Establish security "centres of excellence" in EU universities/research institutes/companies to define best practice professional skills and future needs and a European curriculum schemes (e.g. for cyber skills).
- Implement a Market Analysis Observatory open to EU industry, SMEs, and individual users.
- Foster creation of new funding instruments for exploitation of new technologies, especially by SMEs.
- Create a Scientific, Ethics and Business advisory group on, inter alia, the balance between collective security and privacy technologies

New markets and Emerging/disruptive technologies

- IoE - Internet of Everything
- Big Data
- AI - Artificial Intelligence
- New materials (e.g. *g*raphene)
- Cross-modular education curriculum (combining skills & technologies e.g. through MOOC education)
- Smart personal protective equipment (e.g. wearables, female body armour)
- Autonomy
- Robotics
- Virtual reality (ie. simulation) and miniaturisation
- Synthetic biology.
- Secure and faster delivery for E-commerce

Cross-cutting issues

In segmenting its focus areas to help highlight the research themes that will underpin the next Secure Societies funding rounds, the PASAG has also identified societal concerns and issues that are of a cross-cutting nature and can influence the outcomes of the research, development and innovation programmes. It has also identified and developed an approach to specific enablers that should facilitate the achievement of policy goals embedded in the Horizon 2020 programme.

To date the PASAG has started to analyse the following cross-cutting issues, which are currently ‘works in progress’:

<u>The role of the individual in society</u>

An important common thread in all 5 “Visions” is the need to ensure that the ambition outlined for society, truly reflects and takes into proper account the concerns and the aspirations of the individual citizens that are its fundamental component. For example, individuals, not society, cross borders for legitimate or improper motivations; and individuals value their freedom and their privacy, in ways which may contradict security best practices. We need to understand and preserve these fundamental values while assuring an adequate and supported level of collective security. This will require that law enforcement agencies and security services can continue to be effective in their roles, and continue to be seen not only as a trusted resource to society but to the citizens who treasure their freedom and privacy. As technology becomes increasingly pervasive and indistinct in its access by citizens, law enforcement or perpetrators, it becomes paramount that the bond of trust that enables societal security is reinforced.

Similarly, to ensure society is resilient to disruption, in an environment of uncertainty, the active role of individuals as contributors to security needs to be appropriately encouraged. As such, digital networks represent a significant opportunity, but are also a major challenge. Through them, individual creativity, learning and enterprise can be significantly leveraged to the great benefit of society. But their security can only be assured by a bond of trust between users and enablers, which can be successfully achieved if the relationship is transparent and mindful not only of society but of the rights and objections of the individual.

These factors – and others – signify the importance of maintaining the human factor at the centre of the Horizon 2020 R&D&I programme. The role of the individual should therefore be assessed within the 5 focus areas and how new technologies may impact diverse groups in society. We must also consider new approaches in areas such as social networks, supported by social media, to deepen engagement within sections of society. And we need new approaches 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. This includes advances in identifying risks or threats through visual or technological processes as well as the development of protocols relating to the diverse forms of movement across borders in different locations (airports, large or small ports, etc).

In the area of Fighting Crime and Counter Terrorism gender is relevant in relation to perpetrators and victims of crime and strategies, instruments and processes of counter-terrorism. This includes detection in online and offline environments and networks, and issues of cybersecurity where systems may need to take account of gender characteristics of particular groups of users and contrasting risk factors affecting them. 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.

Secure Societies with increased resilience need to take account of gender through understanding of different ways of engaging, and assessing the impact on, different groups in society. Growing emphasis on live and adaptive responses to crises – whether due to crime, terrorism or natural disaster – needs to consider gender in terms of social roles, risk factors and constraints. Taking account of gender in active citizenship for resilient societies offers possibilities for new approaches and strategies in areas such as community awareness, crisis readiness and management. Technologically driven solutions offer possibilities for building gender sensitivities into social networks in innovative and effective ways to deepen engagement with sections of society. New interdisciplinary research aimed at motivating and empowering different populations to contribute to security societies can usefully take account of gender.

Cybersecurity and Privacy Technologies need to take account of gender in developing more user-friendly and accessible security systems and encouraging individual users in different work, consumer and service environments to be active participants in safeguarding the resilience. Specialized systems in sensitive areas such as health and finance are major spheres of innovation to aid public confidence. Gender aspects of security and privacy risks feature as part of innovation processes recognizing diversity of end-users as part of market segmentation. In this way gender considerations can inform strategies for keeping security and privacy central to digital innovation. In the Internet of Things and Big Data economy the complexity of connections across people, places and things grows exponentially. Gender is one of the key lenses through which new systems, products and services developed.

Growing a Competitive European Security Industry presents a number of challenges linked to wider debates about the need to bring more women into science and technology as well as measures to help them start and grow their own businesses. The fundamental importance of the European security industry to a safe and secure operating environment for EU governments, businesses and the public, underlines the importance of diversity in innovation to harness the best of ideas. There is a need for new security research and industry networks for women across Europe as well as support for engaging more women in innovation in the security sector.

Working Groups

In addition, the PASAG has identified additional themes that may impact the effectiveness of the funding programmes and instruments, the longer-term implications on the practitioner community and industry, and the relationship between security and society. The activity is organised into *ad-hoc* Working Groups, which include:

WG 1: Leveraging R&D&I to develop capability and enhance security industry sub-sectors;

WG 2: Combining existing H2020 procurement tools and resources from EU programmes beyond H2020, and from reinforced EU Agencies in the field of security;

WG 3: Strategically addressing international co-operation in security R&D&I;

WG 4: Achieving the right balance between security and privacy in designing security solutions in a digital-intensive environment;

WG 5: Validating innovative security solutions through processes that take account of practitioners' requirements and citizens' expectations;

WG 6: Optimising access to dual-use R&D&I for civilian security applications;

WG 7: Scenario analysis to identify technological capacity and gaps;

The first three WGs have started their activity and their outline activity is summarised below.

Working Group 1

Implementing new approaches in H2020 based on existing instruments, such as "clusters", could better leverage R&D&I into capability and enhance security industry sub-sectors, optimising future user and market needs.
WG1 proposes to identify conditions, criteria and candidate areas that would benefit from such approaches.

The main objectives of a cluster-like approach would include:

- a short to long term vision in one field or several fields, depending on EU policy requirements and the global market, ensuring both sustainability and flexibility;
- an improved organisation for the selection of the topics in the next calls and overall efficiency of the H2020 security funding and related impact;
- faster processes and accelerated innovation;
- the ability to address policy briefs on specific subjects and promptly answer unexpected and unpredicted threats by calling for expert community support;
- the assurance of neutrality and innovation, also by running parallel competitive solutions in response to specific key topic areas;
- track progress (monitoring of at least the related FP7/H2020 projects main results, with implications for national projects, by a third-party organization/consortium).

This approach should offer a more effective support to industry/SMEs, enabling a more competitive and innovative product and service development cycle, both for the EU market and, possibly, for exports, allowing for more direct links between users, procurement authorities and commercial customers (larger operators, in particular).

Close links need to be established with networks of practitioners, where available, in the field. Active participation of relevant agencies, when possible, would guarantee progress. This can be achieved through an overarching CSA, if recommendations can be collectively approved and implemented.

In addition to the CBRN cluster, already part of the 2016 call, other potential focus areas have been identified based on the following criteria:

- EU Policy driven or, at a minimum, with close policy association;
- sound commercial prospects and competitiveness;
- requirement for an EU level critical mass to address the global market;
- existence and/or opportunity for a coherent community of stakeholders who can work jointly to develop the capabilities and the market;

The first candidate security "cluster" implemented by a CSA and a complementary set of projects is the Border Surveillance sector.

Working Group 2

Procurement tools enabling outstanding technological developments and their efficient transfer into innovation will develop a European Security Industry that is more effective in serving essential users in Europe and internationally. European world-market leaders will deliver superior products and innovative technological solutions both for single tasks and as integrators of capabilities, providing full services for complex security tasks either as single entities or as consortia of European providers.

This will be realised by driving new technologies and their implementation into commercial products and services by enhancing the entrepreneurial environment, incentivising the development of new technology-driven companies and supporting and stimulating SMEs through dedicated funding tools and a procurement strategy that enables follow-through to commercial introduction.

European funding should be appropriately leveraged also to encourage smaller operators to access and exploit existing know-how and technologies developed internally or available within research institutes and universities. Encouraging SMEs to access know-how that is not currently commercialised, and has been generated through public funding in institutes and universities, would not only provide a better route to commercial exploitation, but also stimulate European technology leadership through a European-wide cooperation. Engagement with larger operators that can also fulfil the integrator role, should represent a significant step forward in overcoming the current gap of moving scientific excellence into commercial success.

Procurement tools could enable this innovation through several approaches: (1) supporting SMEs and spin-off companies with dedicated projects covering the transfer of R&D results into innovation, (2) identifying the delivery supply chain at the research programme stage, (3) encouraging procurement of systems and technologies developed within R&D projects, (4) evaluating and testing of the R&D results by a standing group of experts consisting of key users and solution integrators, and finally (5) incentivising academic partners to encourage a successful transfer of R&D results into industrial spin-offs and SMEs that have a demonstrated capability in commercially exploiting R&D outcome.

Working Group 3

The benefits of international research cooperation[7] are well understood, and consequently, openness to third-country cooperation is a baseline characteristic of H2020. These benefits are of particular importance in security research, since

[7] cf. also Horizon 2020 Advisory Group on International Cooperation, Report for the Work Programme 2018-20.

the current global environment is characterised by substantial threats to the security of societies caused by the economic crisis, by turmoil in many areas of the world, including significantly within the EU’s neighbouring areas, and by the resulting refugee crisis. International cooperation is needed to address global threats and challenges that cannot be tackled in isolation. Cooperation in research can trigger developments in other policy areas and in developing and post-crisis regions, as it potentially carries the positive effects of “science diplomacy”. The same is true for the long-term benefits of exporting the EU’s appreciation of fundamental values, such as human rights and the balance between individual freedom, privacy and societal security. However, there are risks to international cooperation which need to be understood and mitigated, in order to maximize the positive impact also for the EU itself: knowledge drainage needs to be prevented; leaking of sensitive information has to be avoided; the EU’s standardization system needs to be protected from being undermined. It is also important to note that EU market fragmentation as well as the lack of inter-MS coordination can be exploited at the cost of EU competitiveness.

Finally, in view of the nature of the security market and related issues linked to end-user involvement, innovation management, and deployment of research results, international cooperation at higher TRL[8] can further complicate EU-internal cooperation. However, the long-lasting tradition in EU-internal cross-border research and security cooperation could also be leveraged to develop cooperation models at a global scale and consequently, help cooperative tackling of global security issues.

[8] Technology Readiness Levels

Annex A

Type A - Individual expert appointed in his/her personal capacity

Name	Nationality	Professional Title	Membership Status
BIESCAS ALTELARREA Leticia	Spain		Member
CANNATACI Joseph A.	Malta		Member
CEUPPENS Inge	Belgium		Member
CREESE Sadie	United Kingdom		Member
DAVEY Caroline	United Kingdom		Member
DE BENEDICTIS Alberto	Italy		Member
GAERTNER Claudia	Germany		Member
HAISMA Ida (until March 2016)	Netherlands		Member
KEARNEY Paul	United Kingdom		Member
KEUS Klaus	Germany		Member
LAMBERT Anne	United Kingdom		Member
LEONE Cristina	Italy		Member
MARTINELLI Fabio	Italy		Member
MISSOWEIT Merle	Germany		Member
NOLLET Jean	France		Member

Dominique			
PADDING Patrick	Netherlands		Member
RAUD Helena	Estonia		Member
RIESCO GRANADINO Raul	Spain		Member
SAMARATI Pierangela	Italy		Member
SANTIAGO CID Maria Elena	Spain		Member
SERREAULT Brigitte	France		Member
SPRONSKA Agnieszka	Poland		Member
SUCHIER Jean-Marc	France		Member
TRAVERS Eleanor	Ireland		Member
TSINISIZELIS Michael	Greece		Member
YOUNGS Gillian	United Kingdom		Member

Type B - Individual expert appointed as representative of a common interest

Name	Nationality	Professional Title	Membership Status
BROEMME Albrecht	Germany		Member
HOEPNER Petra	Germany		Member
LINDBERG Helena	Sweden		Member
REBUFFI Luigi	France		Member