SECURE SOCIETIES

Protecting freedom and security of Europe and its citizens

STRATEGIC RECOMMENDATIONS FOR SECURE SOCIETIES THEME IN HORIZON 2020

Produced by the Secure Societies Advisory Group

December 2015

CONTENTS

1. EXECUTIVE SUMMARY

This document offers strategic recommendations to the European Commission on how the Secure Societies Theme in Horizon 2020 should be developed to address the longer-term priorities and opportunities.

In developing this strategic recommendation the SSAG has considered a wide range of factors including in particular:

- User organisation[1] priorities, indicating where research and innovation is most likely to deliver benefit to important needs and especially anticipating new trends,
- Approaches to the formulation of the Work Programmes that are most appropriate to generate effective outcomes and raise competitiveness of EU industry.

The primary content of this document was prepared by three working groups of the SSAG (2014-2015).

The scope of the Secure Societies theme is very broad and the SSAG looked at several ways to structure the discourse.

It was decided to adopt three broad 'Driver Areas' that together encompass the principal priorities identified by the SSAG.

The term 'Driver' is used in the sense that they represent top-level issues that relate to where innovation is seen to offer substantial benefit. The rationale for these Driver Areas is discussed more fully in Section 4. The three drivers are:

1. **Societal Security & Trust of the Citizen**. This is concerned with ensuring citizens are secure and safe, that they understand and take appropriate action with regard to inevitable risks, and that their perception of security measures is realistic and balances trade-offs with citizens' rights and privacy. This embraces the conventional understanding of national security, including terrorism, but also recognises that members of society are a collective player/stakeholder.

2. **Crime & Crime Prevention**. This addresses a range of important issues relating to crime, its origins and exposure with many trade-offs implied, and that the key challenge is how to reconcile these issues in a practical, ethical and legal way. There is a balance to be made between innovation in responding to crime and approaches that will avoid crime before it occurs.

3. **Data Protection, Resilience and Privacy**. The general area of Cybersecurity faces many challenges, technological, legal, sociological, organisational, integration with physical security, integration with risk management, integration with wider policing and crime prevention, amongst many others. The issues go beyond a narrow definition of ICT to include, for example, physical security, infrastructure control systems, automotive safety, the "internet of things", human behaviour, societal issues and business development needs.

It is emphasised that many technologies and innovations will cut across these outcome-based drivers.

[1] We use the term 'User' to apply to people who actually deploy and operate a capability. The term 'User Organisation' has a broader sense and includes, beyond practitioners, strategy and procurement functions.

The development of Work Programmes for Calls in H2020 should be aware of such potential synergies, for example through the technology roadmapping approach recommended in this Strategy.

It should also be recognised that the detailed impact of cross-cutting technologies and innovative developments will only emerge during the intensive analysis undertaken during the project formulation stages by bidding teams.

A number of key overarching recommendations are offered:

1. There should be a shift towards Work Programmes formulated around broader outcome-driven specifications that can stimulate innovative solutions, with less emphasis on specific technology topics as was the emphasis in FP7.

2. There is need to develop and monitor the *innovation architecture*[2] in topic areas, especially those that depend upon:
   - integration of advances across a number capabilities,
   - where solutions require capabilities to be configured in the context of innovation in user behaviour or process design,
   - or where capabilities support multiple routes to market.

   The SSAG argues for a process to develop and maintain *innovation roadmaps* (including technology roadmapping) that would develop and maintain an explicit view of how research advances in specific capabilities are likely to meet particular market needs, their maturity, and illustrate prospective routes to market.
   This must include consideration of user process change and potential procurement models.

   A suitable term for this is an "*Innovation Roadmapping and Coordination Support Action"* (IRCSA). Each IRCSA would identify key stakeholders and organisations able to be early adopters and would orchestrate co-innovation with users across the related topics. Importantly it would monitor the progress of relevant projects and revise the innovation roadmaps as appropriate throughout the life of H2020.
   The domain of each IRCSA would be designed to cover a priority area of outcomes where integration dependencies are significant, typically this would be a broad area defined together by users and innovation providers.

3. Early consideration should be given to deployment of successful innovation outputs and the identification of early adopters and pilot customers, ideally in the Work Programme Call itself. This is especially true for any topic being considered for PCP/PPP funding models. This may require input and coordination by EU-wide institutions and agencies (such as Europol, FRONTEX) or user networks such as ENLETS to engage potential lead customers as part of the Work Programme development process.

The programme should provide the opportunity for fast-track implementation and deployment to meet urgent needs, recognising the changing and unpredictable nature of security threats, technologies, operational priorities and societal perspectives.

[2] By the term *Innovation Architecture* we mean the way in which a desired outcome, or set of outcomes, can be achieved through multiple and interacting programmes, including the routes to market and procurement aspects. This is closely related to the concept of *Architecting* as defined in systems engineering, for which there is an established literature and methodology. As in the architecture of buildings, this is about how to integrate higher level aspects to achieve objectives, setting the context and rules within which design is conducted.

2. INTRODUCTION

This strategy sets out the approach recommended by the Secure Societies Advisory Group for developing the Work Programmes and the context for future Work Programme Calls in Horizon 2020. The strategy was developed through a series of workshops held primarily in 2014-2015 which defined the overall shape and emphasis of the strategy, supported by three working groups aligned with each of the Drivers that developed the detail under a working group leader for each group, engaging expertise outside the SSAG where appropriate. It should be noted that the role of the SSAG has been to provide advice on the longer-term direction of H2020 activity, not to offer proposals for Work Programme topics. However, in order to provide concrete substance to the strategy, specific areas where topics are envisaged were taken as examples and form an important part of this strategy.

The strategy is influenced by the following observations:

- **Interdependency.** The Secure Societies theme addresses aspects that interact across scientific discovery, technology, the behaviour and concerns of people, processes and training in organisations and of users, and most critically the risks that society faces from malefactors, natural disasters, accidents, etc. Therefore, integration is a critical element of innovation, implying a need to understand the complexity of interactions between the above elements.
- **Complexity.** This complexity needs to be recognised in defining the Work Programme, with an emphasis on setting out objectives and desired outcomes rather than specific requirements for research and innovation topics.
- **Architecting Oversight Process.** A supporting process should be developed as discussed in Section 3 that is able to programme how technologies integrate to address security needs in an evolving way, and provide enduring oversight of innovation and routes to market Horizon 2020 has a priority on pulling through research into capabilities that have a clear route to deployment. This is of special importance in the Secure Societies programme where innovative advances are generally driven by integration of several technologies and definition of new security processes in the context of societal perspectives. The detail of which technologies and security procedures and how they are best integrated, is a complex issue that needs a broad community of expert inputs to be understood. The scope of the interactions will usually extend beyond individual projects.
- **Innovation Roadmapping**. A significant part of the architecting oversight approach should be the development of *innovation roadmaps* that capture the architecture of technologies and societal aspects that address an area of need, linking to potential routes to market and implications for industry competitiveness. An area of need could be a specific area where an overall requirement is being sought, such as land or maritime border security, or they might embrace major elements of the Secure Societies theme. The role of the innovation roadmaps would be to produce a framework to guide the development of a Work Programme Call, and serve as a basis to assist bid teams in their design of proposals and project satisfactory completion, and create an innovation community across the research, industry and user stakeholders. There should be a means to maintain and evolve these innovation roadmaps to reflect progress or difficulties in success of elements, changes in user priorities and evolution of the relevant industries.
- **"CSA Zero" Resourcing.** The process to generate the above innovation roadmaps will need coordination and facilitation. One option is to use the Coordination and Support Action (CSA) instrument to contract for the activities similar to the approach for PCP/PPP programmes, but would be enduring across the H2020 lifetime. Other instruments might also be appropriate, especially in the near term, for example by a

series of workshops supported by the Commission to pilot the techniques in particular areas.

- **User Organisation Engagement.** An important benefit of this process would be early engagement of user organisations and their ability to contribute to the development of solutions. This would therefore provide an effective focus for organisations in Member States to forge mutual understandings as a basis of PPP and PCP initiatives.
- **Upstream and breakthrough Research.** In addition to directed approaches to research and innovation, there is expected to be a need to balance specific fundamental, underpinning or cross-cutting research and innovation that is specific to the needs of the Secure Societies objectives. Examples might include specialised sensors that are not relevant to normal commercial markets, or techniques for offensive Cyber capabilities, specialised techniques for analysing security data, or research into behavioural factors that foster terrorist activity.
- **Fast Track Opportunities.** Innovation requirements are driven in a highly dynamic way by emerging and evolving threat agents. The approach needs to provide an avenue able to respond flexibly to upcoming needs, and to public reactions to events. It must be recognised that the Secure Societies theme is special in having to respond to innovation and opportunism by criminals and adversaries, as well as natural events, against a backdrop of widely available fast moving technology. There must be facility for the programme to respond to new imperatives.
- **Governments-Led Market.** The innovation process in the security field differs from other fields in so far that many aspects are subject to government procurement policies and priorities, and may be subject to regulation. The added value of new security solutions can be difficult to assess by potential procurers, whilst suppliers may lack guidance and vision of the future market opportunities. Both factors can act as strong inertia to innovation and an obstacle to investment. An important element of the programme should be to ensure regulation is devised in a way that promotes innovation, noting the role regulatory instruments can play in promoting innovation, with a linkage between desired objectives and the regulatory agenda. Likewise there should be encouragement for user organisations to adopt approaches that make them receptive to innovation, and for there to be transparent access to enable them to support H2020 projects during their conduct and intercept successful outcomes.

There are also distinctive features of the security market that relate to industry competitiveness: are also the determinants for the main problems that the EU security industry faces:

1. The fragmentation of the EU security market.

   It is widely acknowledged that the EU security market is highly fragmented. There is a lack of harmonized certification procedures and standards across and within Member States, procurement methods differ, timelines vary, communities have different priorities and sensitivities.

   Divergent approaches have effectively led to the creation of different security markets, each of them being split into a large number of security sectors. This not only creates a rather unique situation with respect to the Internal Market, but has also a considerable negative impact on both the supply side (industry) and the demand side (public and private purchasers of security technologies). It leads to high barriers to market entry and makes true economies of scale and access to export markets very difficult, if not impossible.

Much of this fragmentation is inevitable, but H2020 should aim to promote rationalisation of the market as far as possible as far as innovation is concerned.

2. The gap between research and market.

   When performing R&D on new technologies, it is often very difficult for the EU based security industry to predict whether there will be in the end a market uptake, or even to get some sort of reassurance that there will be a market at all. While this is a widespread problem that can also be found across many industrial sectors, it is particularly pertinent for the security industry, which is mostly faced with an institutional market. This leads to a number of negative consequences like for example, potentially promising R&D concepts not being explored, which in turn means that certain technologies that could improve the security of the citizen are not available to the demand side. Conversely, when there is an agreement on the market potential of future products and services, industry should be associated to the R&D topic definition so that these opportunities are supported.

3. Funding Sources for innovation in security

   Security value chains are often complex with many organisations involved and benefits spread widely, for example the security of global supply chains. This presents issues for who should fund innovation and how benefits can provide return to the organisations involved.

4. The societal dimension of security technologies.

   The societal acceptance of new products and technologies is a general challenge across different industrial sectors.

   There are, however, a number of specificities that distinguish security technologies from other areas. Security technologies might directly or indirectly concern fundamental rights, such as the rights for respect for private and family life, protection of personal data, privacy or human dignity.

   The problems associated to the societal acceptance of security technologies results in a number of negative consequences. For industry it means the risk of investing in technologies that are then not accepted by the public, leading to wasted investment. For the demand side it means being forced to purchase a less controversial product that however does not entirely fulfil the security requirements.

3. PROCESS FOR INNOVATION ROADMAPPING

This proposal originates from the SSAG and addresses the need to develop and monitor the *innovation architecture* in topic areas that depend upon:

- integration of advances across a number of capabilities,
- where solutions require capabilities to be configured in the context of user behaviour or process design,
- or where capabilities support multiple routes to market.

The proposal suggests a process to develop an innovation architecture for an area of desired outcomes that would develop and maintain, amongst other things, a technology roadmap linking advances in specific capabilities to particular market needs. This approach has been termed an Innovation Roadmapping and Coordination Support Action (IRCSA). Each IRCSA would show how potential solutions depend upon advances in underpinning capabilities and illustrate prospective routes to market. It would identify key stakeholders and

organisations able to be early adopters. It would orchestrate co-innovation with users. Importantly it would monitor the progress of relevant projects and revise the innovation roadmaps as appropriate for the life of H2020. The domain of each IRCSA would be designed to cover a priority area of outcomes where integration dependencies are significant, typically this would be a broad area defined by users and where research and innovation would lead to a real market.

This approach needs to be an appropriately resourced activity that would involve stakeholders from RTOs and academia, industry and SMEs, users and citizens. It would be enduring over the time H2020 projects remain in progress, able to play a full part in guiding implementation of successful results, and aspect that the SSAG sees as especially important. There may be a number of mechanisms to fund such activities, but a special type of Coordination and Support Actions (CSA) may be the most appropriate. Based on SSAG opinion, these special CSAs would have an advisory role to the Commission, to aid the definition of topics, to bid teams and potential early adopters in the specific domain.

This proposal recognises a number of specific issues arising from experience in FP7[3] that should be considered in maximising the benefit that will be created by H2020 to the security of citizens and the competitiveness of European security industry:

- User engagement. The need to link research and innovation (R&I) more closely with users and their objectives. A feature of innovation in the security area is the importance of co-evolution between technology, human sciences, user processes and behaviours.

- Fragmented topics. Lack of a top-down framework within which innovative capabilities can be drawn together to solve complete problems.

- Limited deployment of integrated solutions. Achieving deployable outcomes can require integration of several advances across capabilities, rather than a single linear project. Beyond the larger demonstration projects, FP7 had limited support to enable teams in complementary projects to integrate individual project outcomes to create and deploy solutions.

- Vague routes to market. The route to market for successful topics can be unclear. In a commercial market the payback from investing in R&I can be assessed in terms of market research and understanding that businesses build internally. In the security area a significant portion of the market is determined by procurement plans and policies in public sector organisations that are difficult to predict with confidence.

- High bid and co-funding costs. Bidding and co-funding costs are high for especially for SMEs and industry and consortia have to make assumptions about the wider context of their proposals and further investment. Greater visibility of the wider innovation landscape in an innovation area would encourage investment and co-funding and lead to better targeted projects. This should be complemented by long term support to excellent teams to reach the maturity and competitiveness required to succeed on the market.

- Poor visibility of achieved outcomes. The achievements of individual projects are not captured in a systematic way, and there is no way to assess how research progress actually delivered is best integrated in wider solutions. There is also no oversight that

[3] FP7 Security Advisory Group Report:
http://ec.europa.eu/research/fp7/pdf/advisory-groups/security_report_2011-2012.pdf#view=fit&pagemode=none….

can advise on options to re-direct research in the list of research progress or lack of it.

The EU Communication COM(2012) 417 "Security Industrial Policy" dated 26th July 2012, highlighted: three distinctive features of the security:

> *"(1)* ***It is a highly fragmented market divided along national or even regional boundaries****. Security, being one of the most sensitive policy fields, is one of the areas where Member States are hesitant to give up their national prerogatives.*
>
> *(2)* ***It is an institutional market****. In large parts the security market is still an institutional market, i.e. the buyers are public authorities. Even in areas where it is a commercial market, the security requirements are still largely framed through legislation.*
>
> *(3)* ***It has a strong societal dimension****. Whilst security is one of the most essential human needs, it is also a highly sensitive area. Security measures and technologies can have an impact on fundamental rights and often provoke fear of a possible undermining of privacy."*

The document also comments:

> *"When performing R&D on new technologies, it is often very difficult for the EU based security industry to predict whether there will be in the end a market uptake, or even to get some sort of reassurance that there will be a market at all. While this is a widespread problem which can also be found across many industrial sectors, it is particularly pertinent for the security industry, which is mostly faced with an institutional market."*

These points support the need for a well-founded top-down and bottom up approach to linking fundamental technology, solution creation and market pull to accelerate innovation that targets priority outcomes and stimulates effective 'innovation chains'.

To address these issues for areas where integration is important, we propose a special form of CSA that provides advice on innovation architecture. Each *Innovation Roadmapping CSA* would cover an area of the Secure Societies programme, not exclusively based on long term research solutions but also addressing mid and short term actions. These areas would be chosen according to a number of criteria, but it is expected that each would cover a broad area or field of interest where a range of capabilities need to be integrated to deliver the desired outcome, or where a common set of capabilities support a range of related needs. The CSAs would be placed competitively under the standard rules, and would address a number of questions:

- What are the main requirements and opportunities in an area?
- What are the driving trends?
- How does research map to produce solutions that meet user and market needs (currently stated and latent) and in what procurement timescales or windows of opportunity exist?
- Are there potential solutions that early adopters would embrace?
- What gaps exist in the current research landscape, and what are the priorities in the short, medium and long term?
- What linkages are relevant to other parts of the H2020 programme?

- What successes are being achieved within relevant projects and is this success being exploited effectively to create impact. Do outcomes from projects require the innovation architecture to be revised?

The Innovation Roadmapping CSA is expected to be led by a core team that would engage industry, research organisations, users and citizens stakeholders, with the opportunity to invite others e.g. NGOs, banks, representatives from related sectors (health etc.). Approaches such as workshops, simulation and surveys would be used to engage wider input as appropriate. The CSAs would be enduring for the H2020 programme, providing advice to the Commission that would also be available to bidders, evaluators and project teams during execution.

There is some similarity between this proposed Innovation Roadmapping CSA and the 'CSA0' that features in PCP projects, but the proposed CSAs would be advisory rather than define tender documents, with a role to inform the wider community, not determine programmes. As such there would be no conflict of interest for entities participating in the IRCSA that might also be bidding into the downstream programme. Of course, one result of the IRCSA process could be the launch of a PCP action.

Note that while CSA appears to be the most appropriate instrument, other funding routes might be considered as alternatives. In the short term a series of Workshops are seen as an appropriate way to develop and test approaches.

The outputs of the Roadmapping CSAs would be:

- Description of the field, real needs, challenges and partners,
- A suitable form of roadmap[4] that shows how different capabilities integrate to produce solutions, and how these solutions are expected to be taken up by users.
- Proposing candidate areas for Research &Innovation activity for future H2020 calls, Programming or cluster approach as mentioned in the SSAG Strategic Vision.
- Identifying candidate new actions, e.g. where there is user support for PCP action, or where the market and position of stakeholders can be strengthened.
- A regular review of progress in projects relevant to its field of interest.
- Indications of where early adopter interest should be stimulated to bring solutions more rapidly to deployment.
- Repository of knowledge and experience, supporting a vibrant innovation community.

It is assumed that future Calls will include topics that aim at broader objectives, instead of or as well as topics that specify specific lines of research and innovation. The 2014 Call has such a mixture of topics types. The Roadmapping CSAs will be especially appropriate to the broader topics. Where possible it would be efficient to group related topics together, but not to make the subject domain too broad as to make the complexity unmanageable. For example, in the draft 2014 Call, the following topics in the 'Fight Against Crime & Terrorism' theme could be candidates:

- Advanced easy to use forensic tools + Internet forensics to combat organised crime
- Securing vehicle supply chains from production to destruction

[4] There are several recognised forms of technology road mapping approaches that could be used. The key feature is the ability to relate advances and maturity in component capabilities to how these might be integrated to generate viable solution products or services, and to show how such solutions would intersect deployment and procurement plans in user organisations.

- All the Urban Security topics
- All the Ethical/Societal Dimension Topics

4. DRIVERS FOR SECURE SOCIETIES WORK PROGRAMME

The scope of the Secure Societies theme is broad and diverse, which raises a question of how to provide a framework for establishing priorities. Many outcomes interact and depend upon overlapping advances. The SSAG decided to structure its analysis by three driver areas that reflect the high-level outcomes. It is recognised that, however the theme is subdivided, there will inevitably be overlaps and ambiguities, but the SSAG offers this framework as one that captures important stakeholder priorities. The SSAG used this framework as the basis for its working groups.

Figure 1 shows the priority innovation challenges that are implied by each driver, and that many challenges have potential to impact upon more than one of the drivers. Each innovation area covers a set of desired outcomes and potential for commercial growth. The SSAG Strategy groups our analysis of the challenges under the dominant driver in each case.

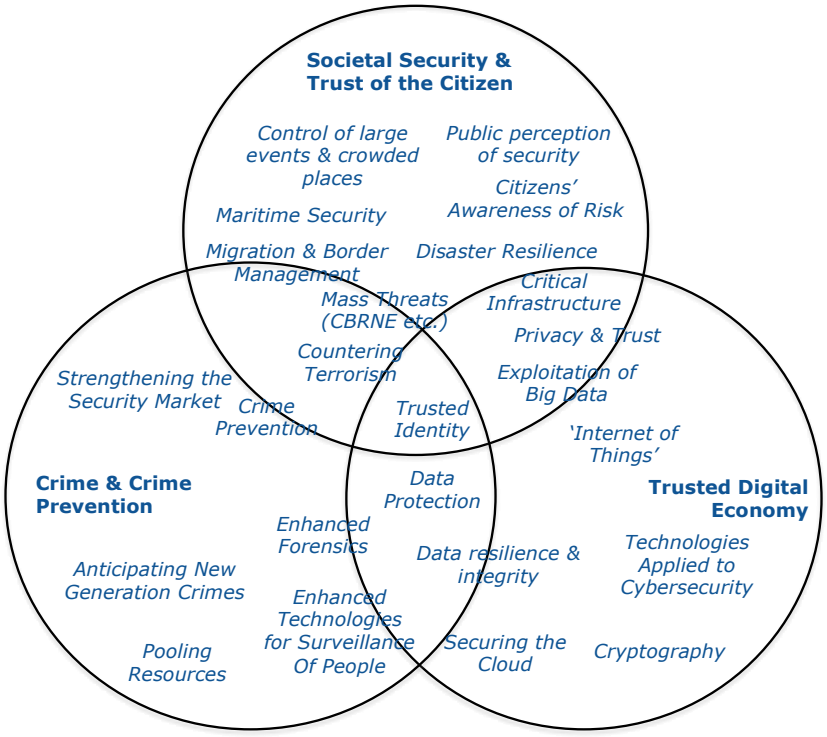

Figure 1 – Drivers of Innovation for Secure Societies with priority innovation areas identified by the SSAG Working Groups.

1. **Societal Security & Trust of the Citizen.** This driver is concerned with ensuring citizens are secure and safe, that they understand and take appropriate action with regard to inevitable risks, and that their perception of security measures is realistic and balances trade-offs with citizens' rights and privacy. This embraces the conventional understanding of national security including terrorism, but also recognises that members of society are a collective player/stakeholder.

2. **Crime & Crime Prevention**. There is a range of important issues relating to crime, its origins and exposure with many trade-offs implied, and that the key challenge is how to reconcile these issues in a practical, ethical and legal way. There is a balance to be made between innovation in responding to crime and approaches that will avoid crime before it occurs.

3. **Trusted Digital Economy**. The general area of Cybersecurity faces many challenges, technological, legal, sociological, organisational, integration with physical security, integration with risk management, integration with wider policing and crime prevention, amongst many others. The issues go beyond the normal definition of ICT to include infrastructure control systems often termed SCADA, automotive safety and what has become known as the "internet of things": the networking of objects of all descriptions. In particular, human behaviour, societal issues and business development needs intersect strongly with innovation in technology. The use of the label "Trusted Digital Economy" has been chosen to emphasise the broadening of Cybersecurity to recognise the societal and business implications, and the associated trade-offs this implies. Effective digital security is becoming a crucial aspect of economic well being and an underpinning for the EU Single Market.

5. DRIVER 1: SOCIETAL SECURITY AND TRUST OF THE CITIZEN

5.1. Public Perception of Security and Citizens Awareness of Risk

Public perception of *security* covers a number of aspects:

- The objective security of members of society,
- Beliefs about the security of oneself and others,
- Subjective security in particular contexts and circumstances,
- Perceptions of the value and appropriateness of security measures.

The short-term challenges would be to address the perception and understanding of *security* in society, as well as feelings and concerns and the behavioural patterns of the citizens. Emotions, beliefs, values and behavioural patterns should be taken into account via a comprehensive summary of the existing studies and research within the field or the currently lacking future research (such as qualitative measurements).

Society members are: (i) users (and also buyers) of the security research and development outputs; and (ii) might be considered the end-users of the solutions in an indirect way — namely as beneficiaries of the results. In addition, taking into account that today's world is getting more and more personalised in terms of goods and services – individuals become very much *self-managed* in a constantly increasing number of aspects of their lives, so soon enough those patterns can also influence the *security* field and the citizens will become even more the direct customers of the *security* products and innovative solutions.

Moreover, the term "society" has changed dramatically (e.g. in many cases the geographical terms are less relevant than shared beliefs) and the "good of the society" as a value is in many cases challenged. The European Societies are composed today of many sub-groups; in some cases tensions exist between the groups. The fact that "public safety" and "public security" are closely interrelated, as well as demand for privacy and individuality, which in many cases is perceived as "competing" with security, are the major factors that need to be addressed in any "*security* related" activity, as those significantly influence the way the public reacts to *security* activities and perceives the security *research* itself.

Members of society should be included in the dialogue about security aspects with end users, industry/SMEs, Research and technology Organisations and policy makers, in order to achieve the common understanding of the needs and requirements for *security* research and its products.

Research into feelings of security has focused on the urban environment — mainly on safety in public places after dark. However, more understanding is required about feelings of *security* in relation to cybercrime, border control, large events, terrorist attacks and disasters. It may be problematic to consider feelings and perceptions of *security* in relation to all types of crime, terrorism, cybercrime, and crisis situations.

Also methodologies for the foresight exercise should be improved. Research on this is so far principally academic and not necessarily applicable in real life. The way the results are being preserved and summarised should also be improved, so the variety of similar studies and projects is not only a collection of questions and answers, but rather gives a comprehensive situational awareness in the field.

Specific requirements will be:

- addressing differences in national and local perceptions of *security* and differences in approaches to *security* amongst different stakeholders;
- the need for citizens to be aware of *security* risks and protect themselves, without feeling afraid unnecessarily; the role of emotions and values in feelings and perceptions of *security*;
- the need for policy makers to understand and respond to citizens' concerns, but not be driven by beliefs that may be misguided, and the role that media and social media play in creating the common perception and understanding of *security*;
- the need to better understand and evaluate the societal impact of *security* measures — this would be beneficial for all stakeholder groups;
- the need to establish policies, mechanisms and measurement tools that promote better security over the longer term, whilst minimising the negative consequences. The research shall be aimed at identification of the main factors influencing the sense of *security/insecurity* within the society and definition of requirements for the means to meet the needs and expectations. It shall cover both the top level/general issues as well as the division to various fields (cyberspace, regular life, big events etc.);
- examining the social trends (e.g. social media) in the context of *security* and the ways they are used and how they influence the shape of the modern society. This shall lead to establishing a common understanding of the *security* within the different stakeholders groups and to a stronger engagement of the citizens in the *security* processes. It may also lay down the foundations for the longer term 'closer to market' innovation strategy;
- addressing the security of the aging population reducing fear and isolation amongst older member of the population living alone; security and wellbeing; security, social inclusion and wellbeing across generations (including children, young people, families, older people);
- trust building – communicating with citizens about security, without undermining trust; fostering social support within urban environments to help improve feelings of security;
- exploring the new appearances of crimes and the connection with organized crime.

The long-term "closer to market" innovation challenge would be to respond to the needs and expectations of the society, taking into account that the constant *personalisation* of goods

and services. Thus, the part of *security* research and innovation, which may lead to an actual implementation of the results, shall be focused on a stronger engagement of the citizens in the security processes – so that *security* (processes and products) is not reserved for special civil or military forces, but the society as an active player in the field as well as the beneficiary and the future direct customer of the innovative solutions.

In parallel, education and training mechanisms should be developed for a whole range of stakeholder groups, including (but not limited to): policy makers; industry; homeowners; architects; urban planners; and city centre managers. The value of technologies in promoting *security*, from both an objective and subjective point of view, and the legal and democratic framework to support them should be critically evaluated.

Strategies to improve the value of technological solutions should be developed and tested, including: integrating technologies within solutions; developing holistic solutions to solve problems, using technology only where necessary and of added value; recognising the value of human interaction in promoting a positive experience and subjective feelings of security.

New innovative products designed for personal use or new ways of using the existing solutions and processes will be the market goal.

5.2. Migration and Border Management

Irregular migration control has been a long-standing concern for the European Union. The main objective is to ensuring an effective control of borders whilst facilitating legitimate travel.

The continuation of political instability and conflict in the Middle East (e.g. Syria, Iraq) and North Africa (Libya) has resulted in mixed flow arrivals, comprised of asylum seekers and irregular migrants, terrorists and victims of trafficking as well as unaccompanied minors.

Management of migratory pressures requires a wide range of measures in which innovation is expected to play an important part. Key issues are likely to be driven by high arrival rates and the need to process people efficiently while respecting their human rights. Identity management in all its forms is likely to be deployed responsively in unconventional locations and environments, including in countries of origin. Means will be required to detect and deter traffickers.

This is an aspect of security where the interplay between developing needs, innovation and operational methods will be very strong. One priority will be developing methods that allow responsive innovation to be initiated and deployed across agencies and Member States. This implies the need for ‘standardisation’, ‘secure cross-border communication’, ‘cross-border access to databases’ etc

Specific areas where activity is needed include support and implementation of the Visa Information System (VIS) for third country nationals, the Schengen Information System (SIS III), Eurodac (EU-wide fingerprint identification system) and the European External Border Surveillance System (EUROSUR), in order to bring together border surveillance systems of the EU Member States into a common cross-border information sharing and analysis system.

Also, developments of technologies and methods to follow and analyse the moving objects and detecting geographic interconnections for understanding the new way of migration (smuggling migrants) and the associated crime shall be envisaged.

This must be complemented by more actions of the EU in support of external security in the affected regions in order to mitigate some migration risks, requiring innovations in policy,

governance, disaster and crisis management, and a more harmonized involvement of the different stakeholders.

5.3. Maritime Security

The maritime domain has important differentiating aspects compared with land border control. These include the need to provide surveillance across large areas of ocean and littoral waters, monitoring long and remote coastlines, the differing imperatives and modus operandi of criminal activity versus illegal migration. Additional issues include piracy, armed robbery at sea, pollution enforcement, security of new forms of economic activity at sea, and fishery regulation.

Specific requirements will be:

- Implementation of rapidly deployable assets, across the EU maritime boundaries; fast mission reconfigurable assets and multi-role services adaptable to various operational needs (technological gap). Development and deployment of RPAS for maritime surveillance, including dedicated payloads. Technologies able to provide synoptic and permanent surveillance (active and passive radars, Electro-optic cameras, etc.). New sensor configuration focusing on satellite constellations for Earth Observation, smaller platforms and new orbits with the aim to improve revisiting time.

- Implementation of cooperative autonomous systems, able to act also in a swarm configuration and diversified mix (aerial vehicles with fix, rotor wings (or tilt-rotor), navigating and submarine autonomous vehicles); innovative C3I systems suitable to effectively control them. Assets for system integration: integration of components in operational command and control centres, providing the needed interface and interoperability for data exchange;

- Creation of enhanced aggregators of information and improved data-fusion models to be adopted in a wider operational scenario; advanced interoperability; resilient and secure “cloud” technologies for data (information) sharing/storing and governance; innovative application interfaces for value added services. Assets for gathering, exchange and data management for public and private users, military or civilian: gathering, control and exchange of information aligned to novel procedures foreseen in the development of the CSDP;

- Development and implementation of Advanced Sensors Technologies (e.g. easily deployable short-range radars or networked acoustic marine detectors); Command and Control (Planning & Mission Support, Decision Support Systems, Diagnostic and Logistic Management); Critical Events Management (Counter Measures, Coordination of manned & unmanned vehicles- air, surface and, underwater systems).

- Implementation of systems, based on GNSS (Global Navigation Satellite Systems) and Satellite Communication solutions, for the provision of value added services designed to support the various maritime users (institutional and civil) during the performance of their functions / in response to the different needs (navigation, control, prevention, etc..), primarily supporting the maritime safety and security. This would exploit the advanced features that Galileo will offer.

- Addressing countermeasures against cyber attacks in maritime context. , There is increasing connection of vessels to the internet (for many different purposes) and in

future there will not only be radar for steering or information exchange; attacks against integrity or availability of any kind of information (e.g. for steering or even for the shipping company; there will be many application areas, viz. the automotive area.

5.4. Protection of Critical Infrastructures

The biggest challenge regarding European critical infrastructures vulnerabilities is creating a common level playing field in Europe. Different Member States (MS) have different interpretations of what should be considered a European Critical Infrastructure (ECI), while private operators have diverse levels of security deployed in their infrastructures, either due to their different national legislative frameworks or due to different risk management, business models and capabilities to invest in up to date and encompassing security.

These gaps should be bridged as this creates a patchwork legislative framework for the protection of critical infrastructures in the EU and lacks a clear direction for the development of better security tools that would help achieve a common level of security throughout Europe. The activities of the ERNCIP[5] form an important basis.

Specific requirements will be:

- European approved risk assessment, risk management and risk mitigation models should be sought in order to rise and align the protection level of critical infrastructures in Europe.
- Technological advanced tools available in the market should meet clear and harmonised standards, creating further certainty in the market and fostering their deployment by MS and operators. Also, the harmonisation of Operator Security Plans, including the link between physical and Cybersecurity, would help the overall improvement of CI security in Europe.
- Given the cross-boundary nature of many critical infrastructures as the effects of their disruption could affect two or more MS, international linkages should be ensured to timely address these effects and their propagation. For this end, a transparent mapping of de facto ECIs should be conducted (not only of the few designated according to the unclear criteria of the Directive[6]). Following this mapping the preventive, protective and resilience measures in place should be assessed for the creation of sector specific and cross sector security models based on best practices and the most advanced technology available. The extant technological needs of MS and operators should be collected based on which standards should be set for new solutions to address these needs and enhance the protection and resilience level.
- Success would consist of having a holistic approach to critical infrastructure protection across Europe, including physical and cyber aspects, with the best available technology deployed allowing for a common level playing field and an alignment of the security level not only between MS, but also between different sectors – *a chain is only as strong as its weakest link*.
- To commonly agree the definition of European Critical Infrastructure that will allow its identification and designation as such, since the definition provided by the Directive has had different interpretations and limited use by MS**.**
- Also the fragmented protection and response measures between by MS, MS owned CI and privately owned CI limits addressing the current vulnerabilities in a harmonised fashion.

[5] European Reference Network for Critical Infrastructure Protection (ERNCIP)
[6] COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

- Finally, more clarity is needed on what is being done to address the current challenges and vulnerabilities of ECIs at EU level, as well as on what should be achieved in concrete terms, and which specific measures are/will be implemented to allow for enhanced security through technological innovation.
- Critical infrastructure protection is interdisciplinary by definition, it includes all sectors of society from transport and energy sectors already addressed in the Directive, to cyber, health, supply chain, etc. Additionally, the effects of a disruption in a CI are likely to have a cross-sector and/or cross-boundary consequence. There is a potential need for better communication between the different operators, a centralised MS point of contact and a working European network of these points of contact. National and European public and private sectors need to have a closer dialogue in constructing new solutions for CIP and a safe platform (which can be an online platform but should also include physical stakeholder meetings) where information can be openly and safely disclosed in a cooperative model. Technical expertise should be pooled so as to present benefits for all sides. Lastly, an environment of trust has to be further developed and stronger links created between the operators and security solutions providers.

5.5. Mass Threats (CBRNe etc.)[7]

The CBRNe field is raising many concerns internally in the EU (risks of nuclear or chemical power plants attacks or disasters, massive digital disruption, dirty bombs, biological food or water contamination etc.) and outside the EU (Sarin attack in Tokyo, CBW attacks in Middle east, in particular in Syria, proliferation). It can take many different forms and is difficult to prevent and identify early enough. It can be accidental and linked with industrial safety, as demonstrated by the Seveso and the Bhopal accidents, or B contamination or it can be deliberate.

A main characteristic of CBRNe, more than any other security threat, is that the CBRNe attacks or disasters are high impact events. High impacts can be in terms of victims (Chernobyl, Fukushima, Syria), activity disruption (AZF in Toulouse) and in all cases, psychological. Such events are escalated and managed by the highest national level, with the support of international authorities such as OPCW and IAAE due to their high visibility.

Member States cooperation in CBRNe is primarily driven by the EU Action Plan on Enhancing the Security of Explosives[8] and the CBRN Action Plan[9] (DG HOME). Other EU policies mention CBRN-e as a priority, namely in the fields of Civil Protection[10] (new Civil Protection Mechanism - DG ECHO), Health and Food Safety[11] (DG SANTE), Energy Infrastructure and Transport Networks[12] (DGs ENER and MOVE), Customs[13] (DG TAXUD),

[7] C, B and R incidents can be linked with explosions and C, B and R threats are aggravated in terms of impacts and response when combined with explosives. In addition, the first hours of an attack may be identified as explosions only, before the C, B or R nature is detected. This is why this topics considers the CBR spectrum, considering explosives if they are linked to CBR events (for contaminant dispersion for instance). It will be referred to as CBRN as it is the most frequent acronym, excluding the N threat (nuclear explosions…), which is considered as out of scope of H2020 (defence issue).

[8] Doc. 8109/08 and Regulation 98/2013

[9] COM(2009) 273 final and COM(2014) 247 final

[10] Decision 1313/2013

[11] Decision 1082/2013

[12] Regulation 347/2013 and Decision 661/2010

[13] COM(2012) 793 final

Environment and Industrial Risks[14] (DG ENV) as well as International Cooperation, e.g. the CBRN Centres of Excellence (Instrument of Stability - DG DEVCO) dedicated to CBRN training and support to third countries.

The relatively low probability but high impact event character of CBRNe makes it difficult to prevent and prepare (there are very variable causes and vulnerabilities, they may cause large crises, and always generate long lasting effects).

As it is not a day to day concern, nor market driven, it is not easy for responders, experts and industry/SMEs/R&D institutions to develop sustainable capabilities during non-crisis time. It is also a burden on operators of large infrastructures or networks among others, as it must so be embedded in the day to day "safety" and build upon the high competencies existing in the continuum safety-security that can only prepare and respond to such events.

Capability building used to be conducted mainly nationally and with limited funding while it has a strong political and communication content, due to the possible huge human and economic impacts.

There is so a need for better capability sharing at the EU level. In particular, the threat perception, communication and response capability throughout Europe are not harmonised (there are different alert thresholds, different means of measurement and forecast).

This is a dual-use field, defence, security and safety that is built on a community of experts in the EU, including industry, SMEs, responders, national reference laboratories and research institutions.

Note that the above factors emphasise the importance of developing an innovation roadmap for this area.

Specific Requirements will be:

- Develop capabilities and innovations in preparedness phase (non-crisis time), while the demand may be limited, through adjacent sectors and markets (such as industrial safety and health) and training;
- Maintain and develop the necessary knowledge and critical technology 'bricks' for a quick settlement in case of a CBRNe event anyhow, based on day-to-day technologies, easy to use interfaces, robotic and automated solutions;
- Improve detection and identification of CB agents (technically and medically), and reduce globally the cost of CBRNe sensors;
- Understand new CBRNe threats that could be introduced by new emerging technologies
    - Nano technologies,
    - Bio technologies,
    - Additive manufacturing,
    - Development of threats in homes,
    - Cyber technologies,
- Better prevent and limit the impacts by CBRNe more resilient infrastructures and networks;

[14] Directive 2012/18/EU

- Balance prevention and recovery. Recovery costs although the event is low probability could have severe economic impact and last for years and even tens of years for RN;
- Support the decision of re-occupancy of an infrastructure after a CBRN event by an improved assessment of threats contamination/decontamination in complex environments urban, indoor etc.: define “How Clean is Clean?” and agreed protocol(s) for identifying when a site is available again for use by the public while the Military/Security Forces will have a different threshold for access;
- The “rare event” nature calls for innovative measures for training and ensuring knowledge retention among responders, as well as risk communication and education of the public under potential risk from CBRN related facilities.

5.6. Control of Large Events and Crowded Places

A major event is characterised by a particular organisational complexity in terms of security, public order, mobility, new lodging, hospitality and health care, with the presence of a large number of personalities and/or participants, and for which it is deemed necessary to take extraordinary measures and urgent. Major events are situations in which a large number of people concentrate in small areas. Moreover, this particular kind of happening involves the attention of worldwide media and broadcasts.

The goal in the management of major events and crowded places is to ensure the ordinary and extraordinary event in an effective and safe way, even in the case of emergencies and crises.

Specific requirements will be:

- Improvement of operation management, offering a centralised overview of the situation in real time;
- Management of information flows, integrating information from sensors and other external data sources to services correlation and presentation in order to provide real-time information for a clear and precise understanding of the situation (Situational Awareness);
- Development of a Decision Support, oriented to the management of the ordinary and extraordinary events, able to provide a specific, efficient and correct handling of the situation;
- Exchange of information between those responsible for the "safety" and "security" by making use of heterogeneous networks, multichannel, and intrinsically safe communications;
- Integration of different sensing technologies to provide the monitoring and surveillance. In this frame, efforts should be focused to build “a toolbox” of different observation technologies, whose integration should be performed so to deal with different infrastructures and type of hazards. The most promising techniques are the ones based on the remote and not-invasive sensing as the electromagnetic and acoustic ones, possibly to be integrated with the usual systems (video surveillance…);
- Development of adaptive Wide Area Surveillance and Monitoring Systems, integrating ground based, airborne and satellite based technologies with navigation technologies and ICT In this way, a new concept of an integrated monitoring should

be developed and tuned to the different types of urban areas, infrastructures and hazards/risks;

- Assuring the interoperability of the different monitoring systems so to allow the information transfer among them and with a command and control centre supervising all the network of the infrastructures and related monitoring systems;
- Definition of common operational monitoring protocols, for the most relevant typologies of infrastructures and risks, so that sensing techniques can be deployed in cascade, depending on the status of the infrastructure and the observed urban scenario;
- Improvement of ICT tools able to control the single monitoring system in order to provide real time information about the "status" of the infrastructures and the urban territory;
- Improvement of the usage of mobile devices both as non-traditional distributed sensors and as ubiquitous and real time information channel for citizens during normal life and crisis events.

A major challenge is the involvement of the citizens in the loop, as providers and users of information. Social Media in crisis offer a crucial communication mechanism to disaster response organisations, first-responders and citizens.

The information shared into social media may be of high-quality: current mobile phones have advanced communications capabilities, including capturing high-definition photos and internet-connectivity that allow uploading photos to a number of social networks and online platforms. Tools such as Facebook, Twitter, etc. have been extensively used to share information, look for specific content e.g. find people or assess the situation. However, the use of these tools should conform to data privacy legislation.

It is fundamental to highlight, in this context, that all those pieces of information should be validated before they are used and integrated in the operational management of the event.

5.7. Disaster Resilience

Disasters can be caused by a variety of reasons, starting from the natural ones, such as those resulting from climate change and ending with the ones caused by the human industrial or agricultural activity[15].

Since the prevention of such lays mostly in the monitoring of the vulnerable areas and prediction of probability of events and consequences, the greatest focus shall be put on preparedness to an immediate response as well as on fast and efficient recovery from the effects on communities and critical infrastructures[16], also from the point of view of a single household.

The EU should be able to respond to disasters both inside and outside the EU. Lessons learnt suggest that there is room for further improvement in terms of efficiency and coherence, rapidity of deployment, operational and political coordination and internal and external visibility of EU actions.

European citizens expect the EU to take measures to protect their lives and assets as well as to provide effective assistance to non-EU countries, as an important expression of European solidarity.

[15] To minimize the effects of disasters, the infrastructure security seeks to limit vulnerability of structures and systems to sabotage, terrorism, information warfare, natural disasters, and contamination, among others.

[16] Critical infrastructures include transport infrastructures, supply chains, hospitals and heath services, network communications, electricity grids, dams, power plants, water systems, among others.

Enhancing Europe's resilience to crises and disasters is one of the core objectives of the Internal Security Strategy in Action, which was adopted in November 2010[17] and has been reinforced in the recent EU agenda on security. The strategy requires solidarity in response and responsibility in prevention and in preparedness, with an emphasis on better EU-level risk assessment and risk management of all potential hazards.

Impacts on supply chains and businesses in private sector shall also be taken into account as they are considered critical infrastructures.

Nowadays supply chains consist of numerous players worldwide and cross and cover various sectors that require continuous innovative business solutions. The development of global supply chains has changed the risk profile of businesses and such global supply structure increases the firms' economic vulnerabilities. In case of disasters and crises, businesses may need coordination through crisis management platforms. Besides, they may need to adopt dynamic models to coordinate the complex networks of supply chains, learn and cope with the consequences as part of corporate responsibility to achieve their resilience and sustainability.

5.8. Countering Terrorism

Countering terrorism depends upon many dimensions and is the subject of large and well-resourced activity by EU Agencies and Member States. There is significant overlap with Crime & Crime Prevention, Societal Security and Trusted Digital Economy driver areas described here. Given this broad and extensive context, H2020 should be responsive to aspects that require fundamental or high risk research where national programmes may be duplicative or sub-critical.

There is also a need for fast-response innovation to mitigate rapidly emergent terrorist modalities. Malicious actors are increasingly able to use advances in technology, methods of persuasion and fund-raising business models. The ability to anticipate and understand new terrorist methods, and to be able to innovate rapidly in response, is a vital systemic capability necessary for successful combating of terrorist actions. H2020 should explore the systemic and organisational implications of providing such suitably responsive innovation ecosystem.

A significant element of R&I for counter terrorism relates to societal factors. Terrorism acts have a wide spectrum of scale and impact – from individual initiatives, driven by the certain personal characteristics combined with ideological and religious views, to organised actions, involving different groups and networks of persons, coming from variety of nations, cultures, religious or political regimes and with a different social status. In both cases, many of those individuals or groups are members of the local communities and citizens of the country they live their everyday life in. Although it may be very challenging, means to define the actual patterns in the behaviour of individuals or processes ruling the formation of such groups or networks shall be examined, in order to develop the "early warning structures", both in terms of societal awareness and reaction (via communication, education, trainings, etc.) as well as technological support (surveillance and alerting systems, internet content monitoring, etc.).

6. DRIVER 2: CRIME AND CRIME PREVENTION

6.1. Crime Prevention

Crime and crime prevention is inter-connected with the other Drivers, but due to its origin this connection is not always technology research related. The necessary response will need an

[17] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0673&from=EN

integrated approach connecting policies, society and technology to strengthen and protect the society as well on European, National, and regional level. Technology is an undisputable enabler and often a game changer in the execution of crime, in crime prevention and in the fight against crime.

European borders are fading: physically, culturally and virtually, a trend that may or may not continue. Due to the speed of geographical and social evolution, and the irreversible causes and uncontrollable effects, national responsible bodies and civilians are confronted with crime and its impact that need inter-Member State alliances and methods. These methods need to provide the Member States with a new level of understanding, recognizing current trends, forecasting new trends, and quick joint and lean responses. A strong alliance will provide a stronger, more harmonised market and clearer routes to market and a safer society.

One of the biggest challenges in crime and crime prevention is the new and emerging ways crimes are spreading in Europe and the way civilians are, or will, be confronted with these societally disruptive crimes. The “new generation of crimes” are not only caused by the facilitating capacity of the Internet, the Internet of things, the increasing usage of new communication, but also caused by a fast changing society.

There is a potential gap in knowledge related to crime. Not only in its appearance, the modus operandi but also in number: Citizens most often do not declare crime unless they suffer financial costs that need to be reimbursed by the insurance companies.

The fast and new appearance of the new generation crimes, or of old crimes in new geographical zones, can be undetectable and unsolvable, with perpetrators who are anonymous unless caught ‘red handed’

When crime is related to serious and organised crime, only direct severe impact (e.g. bank robbery) will be registered. “Smart” serious and organised crime may be unrecognisable, and therefore not foreseen, but has potential to have the highest indirect impact on security, undermining society and the wellbeing of citizens.

When crime is related to the facilitation structure in organisations (organisational crime) the appearances are different and even more undetectable. Examples can be found in the logistic sector, smart drugs, financial markets, brand forgery, underground banking, white collar crime, fraud and in the Cyber area.

Organised Crime Versus Crime In Organisations

Public private partnership is enlarging the capacity in crime fighting: not only to understand the appearances and disruption that is caused by crime. The public private partnership has the potential to execute measures that reduce crime in an effective way. Information sharing, awareness and partnership are key. Crime and crime fighting is not only a responsibility of law enforcement but also of the stakeholders in the public domain.

The direct impact and the usage of new technology to fight or prevent crime needs not only a better understanding but also better skills, knowledge and new best practices in law enforcement to endorse security. Pooling resources on a European level is needed to strengthen dissemination and prevent overlap. The security market can benefit from a set of best practices tested in a real environment to engage the differentiated security market.

Specific Requirements will be:

- Delivery of new methods: implementable for crime reduction and prevention,

- Operational focus: Research that's based on actual operational focus such as the European Multi-disciplinary Crime Threats (EMPACT Priorities) as endorsed by the Council work groups in the European Union. These crime threats are based on the Europol's Serious and Organized Crime Threat Assessment (SOCTA), input for the European Policies[18].
    - **Facilitation of Illegal Immigration** – aiming to: disrupt Organised Crime Groups (OCGs) involved in facilitation of illegal immigration operating in the source countries, at the main entry points to the EU on the main routes and, where evidence based, on alternative channels. To reduce OCGs' abuse of legal channels for migration including the use of fraudulent documents as a means of facilitating illegal immigration.
    - **Trafficking in Human Beings** – aiming to: disrupt OCGs involved in intra-EU human trafficking and human trafficking from the most prevalent external source countries for the purposes of labour exploitation and sexual exploitation; including those groups using Legal Business Structures to facilitate or disguise their criminal activities.
    - **Counterfeit goods** – aiming to: disrupt the OCGs involved in the production and distribution of counterfeit goods violating health, safety and food regulations and those producing sub-standard goods.
    - **Excise and MTIC Fraud** – aiming to: disrupt the capacity of OCGs and specialists involved in excise fraud and Missing Trader Intra Community fraud.
    - **Synthetic Drugs** – aiming to: reduce the production of synthetic drugs in the EU and to disrupt the OCGs involved in synthetic drugs trafficking.
    - **Cocaine and Heroin** – aiming to: reduce cocaine and heroine trafficking to the EU and to disrupt the OCGs facilitating the distribution in the EU.
    - **Illicit Firearms Trafficking** – aiming to: reduce the risk of firearms to the citizen including combating illicit trafficking in firearms.

- Information Exchange Management: Improvement of information sharing, not only through a better exchange between Member States, using LEA's information management systems, but also through new awareness and methods; recognizing crime trends and able to implement prevention methods in Europe.
- Information management: Big data and Open sources are crucial for a better understanding to prevent or fight crime. Understanding the criminal strategies and anticipating trends and the need for new technologies for extracting relevant information out a variety of sources.
- Enhancement of the interoperability between Member States based on legislative agreements and fast track innovative solutions for law enforcement.
- A special focus and research to compete with the fight against cybercrime: raising the awareness from citizens will need a multinational approach and special solutions to protect the right to the Internet. Special resources for supporting the fight against crime enabled on the Internet, based on a 'triple helix' approach are necessary.
- Cloud computing for law enforcement: the need to share secure information and the emerging cloud capacity in the private sector could appear as two opposite parts. Due to the increasing data in law enforcement cooperation research is needed to search for next practices using cloud computing, disabling the current interoperability gaps in information sharing

[18] https://www.europol.europa.eu/content/eu-policy-cycle-empact

- Comprehensive Pre-Commercial procurement and Public Procurement of Innovation for law enforcement: Procurement and tender procedures in law enforcement are challenging, due to low budgets, and a differentiated vendor market without any standards. The low potential to connect with the research technology organisations and industry, to research new opportunities can be better fostered, bringing new technologies and solutions to the market. In recent years law enforcement was not successful to take up this vested interested. A divergent approach needs to be implemented to use PCP/PPI for crime and crime prevention. Specific PCP / PPI law enforcement actions, connected with operational needs shall enhance the technology capability and harmonisation of usage.
- Technologies and social sciences methods (approaches) that help understanding how organised crime exploits socio-economic conditions for the crime actors benefit.
- Enhanced technologies for surveillance (CCAT) and image processing, fast and reliable identification of object.
- An European framework regarding the usage of new technologies with a balance in effective measures and privacy protection based on legislation

6.2. Anticipating New Generation Crimes

New forms of crime are seen as an emerging spreading phenomenon. To protect civilians and economy, this needs a compendium of methods for preventing and fighting crime. An example is the unbounded appearance of crimes exploiting the Internet. Another new appearance is caused by the (not foreseen) crime related to the auxiliary structure of an open Europe, enabling the free transport of people and goods. This addresses a cross cutting new challenge where European Directorate Generals (DG's) such as DG HOME, DG MOVE, DG REGIO, DG GROW and DG OLAF could be partners to be aligned, but also with the Member States. Member States are confronted with the impact of travelling criminals, causing high impact or high volume crime, or, without any physical travelling, will be confronted with new ways of fraud, threads.

Crime fighting and prevention tend to be implemented in traditional ways. This low flexibility is a risk that needs to be addressed. The adaptability for new solutions is low due to the hierarchical structure and fixed and insufficient budgets. The fight against crime and crime prevention will need flexible and measures implemented rapidly, with the resources required and justified within discussions on competence and ethical rules. Solutions needs to relate to "real case scenarios", recognisable for European and National Policy makers, but above all to the leaders of law enforcement.

Specific Requirements will be:

- Forecasting and understanding fast appearing or potential new crimes,
- Technologies that can anticipate the impact of new trends, upcoming crimes and potential threats (tools for Knowledge and Data Management, Tools for efficient Big Data analysis and Linked Data). The challenge and objective in pursuing these technologies is to discover the rapidly evolving trends, to enable development of new mobile and flexible methods for identifying group structures and alliances, multi-crime and different crime activities. Their use should enable understanding and detecting the dynamics of the potential threats and crimes in a sufficiently anticipatory manner in order to be able to act in time and appropriately.

- Strong coordination to enforce cooperation and rapid response on crimes that appear on the European level and, or crimes that appear in new geographical zones.

6.3. Relationship between European policy and crime to strengthen the security market

At the European and national level, policies are made to secure the society and to fight crime. To build a secure society law enforcement will need new capabilities enabled by new technologies.

The Internal Security Funds (to implement the Internal Security Strategy), H2020 ‘s Industrial Policy (to strengthen the industrial competiveness) and Structural and Regional funds are potential sources for the enhanced Security of Citizens. A coalition in execution and governance is needed to prevent further fragmentation in the Security domain. Deliverables and results can be integrated and exploited. Short, mid and long term needs to fight crime and activate crime prevention can be better harmonized by using the objectives of the funds. (feed-in/feed-out).

The end user involvement in the security domain is fragile whenever it comes to implementing new technologies. The operational needs are demanding direct useable technology, or technology with a high technology readiness level.

A coherent market could benefit of:

- Policy that will integrate the use of technology, defining needs in specific areas. Without supporting boundary conditions for technology the execution of the policy will be not comprehensive.This will need a “state of play”, defining what is currently available to execute the policy and what is needed, to roadmap the technological capabilities. Different areas of technology interest can be defined from sensor to cybercrime tools.

- Approved technology, tested on its integrity and transparency. The pledge is to define an approval procedure that enables law enforcement to use these tools in their investigations based on solid legislation such as a warrant. This will include privacy enhancing technologies, anti-tampering protection and data protection. It will push the market towards more standards and procedures and is a proven method to have a transparent way of using technologies based on a chain of custody.

- Legislation: The use of technology to fight crime is in each Member State based on the National legislation. European treaties apply to share information and to cooperate. There is currently no overarching European legislation that is open enough to integrate the National legislative rules to apply technology. To harmonize standards and to have an effective inter-operability, new rules need to be set to safeguard the implementation of technology in the fight against crime. The European legislation will strongly refer to the above mentioned need for approved technology. Additional national requirements to use the equipment can be integrated based on *privacy by design*, and provisioning (e.g. based on warrant where the public prosecutor will define the use and conditions to use the technology).

6.4. Pooling resources: the European Law Enforcement Cooperation.

The establishment of a strong European law enforcement platform with a wide applicability to a wide range of technology is needed. The SSAG’s advice to use Innovation Roadmap Coordination Support Actions in this area looks opportune due to the direct link with the

European Security Strategy, operational needs, the connection with European Law Enforcement Agencies and the availability of a coherent market. An IRCSA can be established using the existing European LEA partners to build a European Ecosystem for Law Enforcement.

This ecosystem can establish user groups based on operational needs, integrate present research, activate new research and define gaps, define areas for standardisation and connect policy and technology.

6.5. Forensics

Forensics offers a wide range of tools for investigators to utilise in the prevention and detection of criminal activity. The significant advantage with many other types of information is that forensics provides hard scientific evidence that originates from a validated source that is accepted by the courts. The disadvantage is that it is almost exclusively used in a reactive manner, i.e. post event, and there are opportunities to consider how forensics can be used in a predictive manner to prevent crime and provide improved intelligence opportunities to LEA's.

Areas of forensics are utilising transferrable science and technology from other domains, such as health, defence, and ICT as examples where opportunities can be developed to meet an operational need. There are however, further areas for development that are still to be exploited such as the information that is available from biological material where we are currently using it to identify an individual, but modern genomic technology offers potential for much more intelligence information about appearance, traits and lifestyle.

Advances in technology bring a drive for faster forensics that is leading towards improved capability closer to the crime scene. The traditional methods for trace evidence location and recovery are tried and tested, but can be time consuming and requires evidence being moved over large geographical areas for the analysis stage. Miniaturisation of technology and the further development of the "lab on a chip" concept will enable more analytical activity to be carried out at, or closer to the scene without the need for laboratory analysis.

This trend will include more automation and interpretation of information by the machine rather than the human. The vision of electronic recovery of finger marks from crime scenes that are transmitted to databases, searched and identified and returned to investigators without any human intervention will become a reality in the not too distant future. This will require the fusion of the science and technology to enable this to become operationally viable.

Some detailed examples of future opportunities for improved use of forensics are:

- Rapid DNA technology has been on the horizon for a number of years, but is now a reality that needs to be harnessed in a structured way that provides faster interventions and capabilities. The introduction of such technology should not be allowed to compromise the "gold standard" of DNA evidence that has been subject to thorough and robust scrutiny. In addition, the potential of automating the comparison process will reduce human error and prove to be a more cost effective means of delivering services. The vision of uploading a crime scene stain directly from the scene into an automated process should be explored fully.
- The explosion of new psychoactive and substances of abuse provide an operational need for earlier intervention through rapid analytical capability. In essence, we need to bring that analytical capability close to the point of recovery so that it can be dealt with to evidential standards in an operational environment, rather than an analytical laboratory.

- Advances in sensor and photonic technology utilised in other sectors need to be adapted and transferred into the forensics arena. They do however need to be validated techniques that can be accepted by the courts. This includes hyper and multi spectral imaging methods that are used in limited applications but offer further potential, as well as a range of sensor technology that is yet to be fully exploited.
- There is limited availability of current reference databases that can be used for research and development purposes. This includes biometric reference sources and also studies around persistence that are of no real commercial value but provide academia and industry with essential access to real life case data.

Whilst the traditional forensic activity supports LEA's, the emerging demands of digital forensics continue to challenge all operating in this field. For the purposes of this document, digital forensics is the recovery of information, and not the investigation of online crime. Most crime scenes or detained persons have a digital footprint, whether it is a mobile telephone or CCTV footage, they all offer investigative opportunities irrespective of where the data is stored.

The significant challenge is the volume of data that needs to be recovered and then examined for relevant information that can assist LEA's. This offers a number of issues to be addressed starting with the recovery stage. Increasingly, digital forensic evidence is recovered through the use of automated commercially available tools, and these tools will frequently be used by front-line officers, i.e. those without specialist digital forensics training. This will increase the reliance on these tools to produce evidence that can be relied on in court. The challenge is to ensure that these tools can keep pace with the rate of technological change and robustly quality assured to provide confidence in their provenance.

Increasingly LEA's are facing cloud based evidence storage, where the relevant digital evidence may not be stored on the physical device at the crime scene but be online, and therefore in another (or uncertain) jurisdiction. The connection might be password protected, but may, if the suspect is apprehended in the act, be open and easily accessible, but perhaps only for a short time. The legality of its recovery from outside a home jurisdiction presents interesting legal challenges posing the question, can it be legally recovered? Accessibility of cloud based storage requires a different approach than conventional recovery techniques and early developmental work has offered promising results but there is still significant progress to be made in this area, offering specialist commercial partners opportunities to partner with LEA's.

Given the rapidly increasing volume of data stored, it is not always practical (or proportionate?) to undertake a full forensic examination of all digital data on a device or devices in a particular case. There will be associated risks in undertaking a partial/prioritized examination and how does this compare to the risks of delays/queuing for a full examination? The volumes of digital investigations now required as part of conventional criminal activity is outstripping demand, and the more sophisticated organised crime groups are becoming more forensically aware to the techniques used by LEA's. Improved capability is required to enhance the ability of LEA's to address the problem of both conventional crime committed using digital technology as well as digitally enable crime.

Due to new technologies in other domains, such as the health sector, the traditional crime scene assessment methods evolved the last 5 years. The search for fingerprints, DNA and other traces profits from new capabilities. The expansion of new methods and technology is stressed to apply more in situ technologies. This implies the need of other technologies for data storage and transmission.

7. DRIVER 3: TRUSTED DIGITAL ECONOMY

The general area of Cybersecurity faces many challenges, technological, legal, sociological, organisational, integration with physical security, integration with risk management, integration with wider policing and crime prevention, amongst many others. Digital security is also a critical factor in the success of business and the needs of the European Single Market. The issues go beyond the normal definition of ICT to include SCADA control systems, automotive safety and what is known as the “internet of things”, the networking of objects of all descriptions. In particular, human behaviour, societal issues and business development needs intersect strongly with innovation in technology.

While there are major technology challenges, for example how to achieve stronger end-to-end security in services and updating the underlying internet security architecture, we see the biggest immediate issues to be around how technology is implemented in organisations’ processes and its external portals, with human behaviours that is ethically and legally viable. In the following, we give examples of areas where new research and innovation is seen as being required.

This subject involves a plethora of tough problems. This arises because of the close interrelation between technology and societal factors, and the difficulties of translating ethical constraints into practical solutions. Its close relationship with national security, policing, social media, corporate e-business practices and criminality makes for a very challenging context. There is a very strong need for fresh avenues of research to make progress in this difficult area where multi-disciplinary teams and projects that integrate capabilities will play a major part.

Many opportunities for a multifaceted approach to Cybersecurity research exist around ownership, identity, privacy, measuring trust, valuing digital interactions and evaluating public persuasion factors, however the group identified specific and practical steps that research organisations should take to address the Cybersecurity opportunities. Social norms and users should be studied to assess how to deliver Cybersecurity information.

Cyber space policies, generated and set down by governments, should be accompanied by Cybersecurity research to influence the development of such policies and regulations. The impact of cyber and other legislation should be taken into account in researching Cybersecurity and again Cybersecurity research needs to influence the development of such legislation. The economics of Cybersecurity is important, development of effective security may only take place if it is economical to do so, this facet of cyber space needs to be studied and solutions suggested.

A framework should be developed to allow policy makers to understand the implications of their policies and research should be identified that can be used to inform Cybersecurity policies. Finally, public sector Cybersecurity needs and solutions should be centralised and aggregated.

Privacy and security (especially privacy) are subjective characteristics, perceived differently by each person with differing norms across communities and nations. There is an inevitable dilemma between the need to allow companies to create value from personal information whilst giving users adequate privacy. Similarly with security interests: companies (pressure to reduce security costs) vs. citizens (want applications as secure as possible). A key bottleneck will be how to oversee or regulate this balance in a way that is scalable, efficient and independent.

A strong emphasis on security and privacy in the early phases of research and innovation project will certainly add complexity, however, if taking into account the whole lifecycle of new products, services or business development, the earlier security and privacy will be developed, analysed and guaranteed, the easier innovation will be put on the market and accepted by consumers and the society.

A particular issue in digital trust is the fact that many risks arise because of determined malicious malefactors able to exploit opportunistically gaps in capability. Unlike standard risk management, we face innovative forces seeking unforeseen vulnerabilities. Hence it is difficult to develop strategies and technologies in time. For this reason self-adapting/self-healing systems are proposed that can "learn" how to protect and react. In addition "good" technologies can often be used oppositional, e.g. monitoring vs. surveillance. Research on how to constrain the "usage" of innovations for the intended purpose is a challenge.

Sharing data securely and protecting privacy are manifestly huge issues affecting the public at large, business, governments and political debate. Technological aspects are fundamental, but the most challenging issues arise from the way technology, business processes and human behaviour intersect, and it is in this area that important and rapid progress can be made through research and innovation.

All aspects of Cybersecurity have to be better understood by society. Methods and tools have to be adopted by the different stakeholders to better decide which assets (data, keys, systems etc.) they have to protect and how to conduct and assess the risk management implications. This suggests an emphasis on independent certification, trust marks with confidence on objects or services, regulations in specific areas to enforce security and privacy management, means to raise awareness and public engagement, etc.

Two amongst several driving trends are the pace of the penetration of mobile Internet and the security issues arising from the use of mobile devices, and the extension of digital access into non-generic systems including automotive, SCADA (supervisory control and data acquisition) and "the internet of things".

H2020 Research & Innovation projects should be able to create the foundations that support:

- Solutions that optimally integrate technology capabilities with human behaviours and legal frameworks,
- Guidance and regulations that strengthen information governance in society and organisations;
- Illuminate understanding of how to balance privacy against needs of national security or benefits from Big Data,
- Future Internet applications that adapt to particular user needs, that do not perform in the same for all users, but which can still be shown to comply with data protection and privacy standards and regulations,
- Lightweight security protocols for moving objects with low power capacities (mobile devices, vehicles, cameras and other sensor devices that are connected via wireless networks),
- Next generation identities, i.e. partial identities (e.g identities depending on a specific context), new forms of pseudonymity and anonymity to ensure privacy, identification and authentication methods not only for persons, but also for objects and services to assure that the interactions are performed with the intended counterpart. This is likely to stimulate development of new legal frameworks that, for example, provide limitation on service provider liabilities,

- Dynamic adaptability of systems to new and changing risks, i.e. recognizing the risk and learning how to adapt itself intelligent and thereby automatically strengthen resilience,
- Privacy-enhancing technologies that are easy to use and are also respected and enforced internationally,
- Solutions empowering users and data owners to effectively control their own data,
- Dependability management strategies, technologies, mechanisms, and systems to ensure resilience and service continuity,
- Strategies and mechanisms to select and tailor the dependability solution on the specific application needs defined by Service Level Agreements,
- The issues covered here are fundamentally of a global, involving technology, behaviours, legal frameworks and political initiatives that necessarily need to have coherence across EU Member States. These are also issues that have a profound impact on the effectiveness of businesses and the well-being of citizens, and are areas where EU nations need to able to have coordinated influence. The digital world has been dominated by the US for the past 3 decades, and this has given US organisations a significant advantage. This is despite EU experts frequently having an influential personal role in the formulation of standards, for example through the Internet Engineering Task Force (the IETF). In the future it is important that the EU has increased influence and innovation momentum in the digital area, especially given the technological prowess of emerging economic areas.

The NIS WG3 Research Landscape deliverable[19] provides a useful analysis of issues and trends in Cybersecurity research, and describes of the state of the art in each. They are listed below, re-grouped under three main headings:

1. Innovations in technology and business, leisure and other practices requiring a new approach to security:
   a. Internet of things
   b. Cloud
   c. Big Data
   d. e-Government
   e. Banking and finance
   f. Smart cities
   g. Telecommunications/ICT services

2. Open social, technical and other challenges, requirements and threats for which technical solutions may provide answers:
   a. Software security and secure software development
   b. Network and mobile security
   c. Cybersecurity threat technologies/ Offensive technologies
   d. Data Protection
   e. Cybersecurity awareness and training
   f. Military and defence
   g. Food
   h. Drinking water and water treatment systems
   i. Agriculture

[19] STATE-OF-THE-ART of SECURE ICT LANDSCAPE (FINAL, VERSION 1), July 2014, NIS Platform Working Group 3, ed. Kert, Lopez, Markatos, Preneel

3. Security technologies and concepts: lists the following security technologies and describes the state of the art in each:
   a. Metrics in Cybersecurity
   b. Authentication, Authorization and Access Control
   c. System integrity -– Antivirus – Antispyware
   d. Cryptology
   e. Audit and monitoring
   f. Configuration Management and Assurance
   g. Hardware and platform security
   h. Information Sharing technologies

7.1. Data Security and Protection

Data security and protection include a general view of how data can be protected from unauthorised access or damage while enabling desired sharing. This includes underlying IT security but is seen as how data, the services that use data, and the way people need to share data as the driving factors. Note that this includes the narrower area of protecting ICT systems from attack, but looks wider to how data can be managed in a way that gives it the required protection in all aspects of the context of its use.

Specific requirements will be:

- Improving protection of data held in mobile devices and their use in everyday life, administration, services and managing the infrastructure. The security for those devices is not sufficiently developed to address threats including data breaches, interceptions, fraud, and identity theft,
- Means to generate widespread adoption of best practice security and in the holding of data, encouraging stronger information governance in organisations, technical control, and possible greater regulation, with norms on compensation and redress.
- Techniques to enable security to be designed in from the outset. Many new services are introduced from a technology- or service-push origination with security added later as risks emerge. Instead, we need innovators to build security into their solutions from the start. The established terms “security by design” and “security by default” describe this area, the key issue is how these can be economically encompassed into the innovation models that are adopted, especially by SMEs, and as ‘the internet of things’ grows.
- Security of services and data must be facilitated assuming wider sharing and access to data, including across insecure systems, networks and cloud services. Protection needs to be at the data level as well as across systems. The “shielding principle” (build a fortress) does not work anymore (e.g. firewalls, secure networks, secure routers).
- Non-Specialist end-users need a means to give some confidence guarantee that a service that accesses their data is valid and safe. Europe, because of its large market and advanced institutions, is in an especially good position to develop and deploy techniques that enable independent validation and certification of services and data.
- A significant challenge is enabling businesses to counter cyber attacks, which may come from global competitors, organised crime or “hacktivists”. Many companies,

especially SMEs, are vulnerable through weak security measures and poor workforce culture. This vulnerability can cause substantial harm to companies, for example loss of key intellectual property.

- A very significant challenge is how safety, security and quality grow together and influence each other as networked data pervades across systems. The dependencies on each have to be explored deeply.
- The rating or measurement of the security of an overall system is only rudimentary with traditional methods. Security-by-design, risk surveillance, security testing, certification, monitoring of processes are all isolated activities to provide more secure systems. Yet continuous and integrated criteria, concepts and processes to certify security are missing.
- Information sharing including exchanging of experiences is a high challenging issue in Cybersecurity. There is a strong need to install procedures, technologies and infrastructures (platform) to ensure a secure and reliable exchange.
- Cybersecurity related practice oriented information, composed with forecasting information build a central building block to ensure appropriate and adequate reaction and prevention.
- Malware analysis: during the process of analysing malware it is necessary to extract possible information e.g. about the way of attacking to establish or deploy adequate countermeasures, to investigate the attack in respect to the attacker or originator opening the possibility to start possible prosecution. The evolution of attacking technologies, techniques and related procedures require new kind of technological and legal countermeasures, embedded in comprehensive solutions.
- Valuation of Digital Interactions: identifying the importance of and the value of assets, classifying the security required for an asset based on its value and the development of an asset currency (e.g. personal information currency) would be necessary. Can different levels of security be developed for different interactions involving differently valued assets, e.g. different personal information assets?
- Cyber space is a very good tool to damage or destroy enemies. It is relatively simple to develop cyber weapons compared with conventional weapons. Cyber war attacks can be against communications or enough smart phones to disrupt a network, for a relatively small amount of money. Cyber war attacks can also be against critical infrastructures. There is a need to introduce secure operating systems to these that will require a redesign of operational software. Moreover, international agreements for the control of cyber weapons have to be implemented.
- Holistic Mobile Security Models. Security breaches in the mobile ecosystem can have many sources, including handset vulnerabilities, operating system flaws, malicious applications and even network availability. As a result, no single player in the ecosystem can have sole responsibility for security. Research in the mobile space should look first of all at holistic security models, and investigate common policies and technologies that can be applied to all components and players in the mobile architecture.
- Trust models for the consumer. The issue of trust has a significant impact on consumer confidence regarding the management of their confidential data and the uptake of applications like secure mobile banking. From the consumer point of view, there are still dangers inherent in the transmission of private transactions and the storing of sensitive data by service providers. Research should focus on trust models, authentication and application certification in order that consumers can manage sensitive data and carry out secure transactions with confidence. As part of the trust models, pan-European models for service providers claiming the data

protection and security features of their services are needed. These models will allow the benchmarking of services and technology solutions according to the offered protection level and will allow transparency in the selection of providers and in accountability control.

- For businesses, the distribution of data across the mobile ecosystem and into the enterprise also creates questions of ownership, responsibility and control. This is compounded by the complexity of a Bring Your Own Device (BYOD) environment, where such issues extend to both the data and the device. From an enterprise perspective, research should examine problems such as data segregation, filtering, configuration and control in order to enable corporations to implement a BYOD model which is both secure and reliable.
- The key to success in this area is that any research must consider the views and needs of all stakeholders in the ecosystem, as well as the input of consumers, businesses, legislators and regulators.
- Contributions to a more secure transport network. For example, in the future context of the air transport network and the concept of single sky, SWIM (System Wide Information Management) will manage the traffic management. The exchange of data during a flight has to be also secured[20] but it is also necessary to improve the protection of data exchanged during landing or preparation of take-off operations between key stakeholders (pilot, responsible of areas around airplanes, C2 airlines centres) in airports

7.2. Privacy and Trust

Privacy includes the means to enable citizens to have appropriate protection of private data whilst recognising the inevitable and generally desirable accumulation of information that is possible in the cyber world.

Citizens are concerned about the consequences of sharing their private data with powerful companies/organisations that can use them to learn about mass trends, mass behaviour, etc.

How citizens can be empowered with automated tools to still provide exciting services while retaining control over private data, yet still supporting appropriate business models for providers.

The emerging and ever growing trend of mobile systems and the Internet of Things, are naturally introducing a scenario where an enormous amount of user data is being stored and processed by third parties, with users losing control over their own data.

Growth in the use of Cloud services and Software as a Service (SaaS), especially its rapid uptake by business, poses new contractual and legal challenges for protecting and sharing data, for example across an international supply chain.

The provisions for privacy that apply in the physical world should be used in the digital world.

- *How much data is on the Internet about you?*
- *Why are we forced to post our data to obtain many computer services?*

Future technologies required to tackle the opportunities in Cybersecurity included various machine learning techniques for cyber space to build trust, model attacks, isolate attacks

[20] Actions covered by SESAR

and attack recovery. Furthermore, more government regulations are needed for the protection of privacy in the digital world.

Specific Requirements will be:

- Cloud based applications that are able to keep track on the needs in security and privacy of the users for all their data deployed on different providers with different policies. Platforms that are able to enforce the user privacy and security needs/options/policies on other applications i.e. change the behaviour of the other application.
- Techniques to control exploitation of private data by “Big Data”. This shows an exponential rise, yet privacy arrangements in social media and other public repositories are fragmented and largely immature.
- New needs for IT-forensics/future video analysis in the field of video data (mass video analysing including automatic analyse of video data, intelligent pattern recognition, conversion of formats, interoperability etc.) without conflicting privacy issues
- Studies of social norms particularly internationally and studies with users to assess how to deliver Cybersecurity information.
- Identification of policies based on results, identification of research that can be used to inform Cybersecurity policies, development of a framework for allowing policy makers to understand the implications of their policies.
- Bringing together of public sector that have Cybersecurity needs and research and commercial players that have developed security solutions, emulate the health sector in looking at areas where behaviour is restricting Cybersecurity improvement.

7.3. Resilience and Integrity

Data is vital to the effective delivery of almost every aspect of life and often to safety. Changes in the way data is stored and accessed, including the impact of mobile devices and ‘Internet of things’, impact upon how to ensure availability in the event of disruption.

Specific requirements will be:

- With the increasing amount of sensitive data it is important to avoid data loss in order to be able to continue operating in the event of some kind of disruption, whether it is a breakdown of equipment, a power outage or even a natural disaster. Cloud computing solutions and architectures are capable of both protecting against and dealing with a potential catastrophe, offering resiliency capacities through redundant implementation. However a mix of physical and virtual infrastructures, using the cloud for disaster recovery is not just a case of simply replicating data as it largely depends on the size and scope of the production workloads to be protected, and selecting the disaster recovery solution that is the most suitable for its replication. It is essential that key issues are addressed early on to ensure the infrastructures work together advancing and acquiring deep knowledge on the multi-cloud and mobile cloud architectures paradigms.
- Resilience in respect to technologies and infrastructures are new technical challenges (in IT and IT security it includes e.g. intelligent networks (incl. SDN), self learning elements and tools, e.g. decision tools (for operators), network components). A future solution might be “resilience–by-design”.
- Measuring resilience including underlying criteria remains a challenge. We need a complete new understanding and meaning of resilience in data management.

- Resilience in cascading effects in respect e.g. to attacks and upcoming/moving threat environments are complex scenarios, which need further research and innovation.
- Resilience has to be seen in the context to environment conditions, i.e. resilience solutions are not “one-size-fits-it-all” solutions.
- Measurement of Trust. Trust in cyber space is very important but the key question is how trust can be measured. *Is it possible to develop acceptable trust metrics and Cybersecurity features that increase trust?* Trust and assurance sources are key, e.g. assurance from the source of friends is much more likely to influence people to take-up security features.
- We need more scenario-based approaches in resilience that will open the opportunity for “simulation approaches”; this should be enhanced by more demonstrations and trials.

7.4. Trusted Identity

The identification of persons, organisations, systems, things, services or non-material goods are a pre-requisite for a secure and reliable communication and service usage. Authentication, authorisation and accountability rely on identities. A trusted identity may be proven by different means (for people e.g. ID cards, biometrics, signature certificates or a pseudonyms). For non-human identities other trusted capabilities or attributes have to be provided that constitute an identity. Methods for identifying objects or things are still largely unexplored. Novel technologies may for example determine identities of objects based on shapes or materials.

Specific requirements will be:

- Introduction of a widespread introduction of scalable public key infrastructure at citizen level, a breakthrough in authentication technology and how people use it, or common standards on ethical implications of data accumulation,
- Enhanced biometrical authentication methods that are easy to use but also revocable might reduce need for various existing methods,
- Further developments of wearable systems (maybe we do then not need the mobile anymore) or even implantation of chips when born might raise even more privacy problems. But on the other hand the mental attitude towards privacy changes in the next generations.
- Identity and Privacy. A great deal of behaviour in cyber space depends on who we think we are interacting with, trust in online identity is very important. Mechanisms for providing identity need to be publicly acceptable and need to consider privacy. For example, is identification necessary for identity and is it possible to have pseudo private identities i.e. a trusted identity online that is different from that in the physical domain?
- The creation, selection and handling of different identities by citizens (partial identities, pseudonyms, anonymous) and their context-specific usage has to be simple and secure.

7.5. Exploitation of Big Data

The term Big Data refers to a collection of techniques and technologies designed to handle data that is characterised by the ‘3 Vs’, i.e. it has high **V**olume (the number of records or documents in a collection is very large), **V**elocity (new data is being added to the collection

at a rapid rate) and **V**ariety (the collection contains structured and unstructured data from many different sources and in many different formats).

Large amounts of data are already being collected in the course of providing on-line services and operating information and communication system, and the availability of low-cost storage makes it economical to retain them. Trends such as the Internet of Things (see 7.6) are likely to increase these amounts dramatically. The motivation behind Big Data technology is to release the valuable information that is latent in such large collections by analysing trends, correlating behaviours, applying machine learning techniques, etc. in order, for example, to understand customer behaviours and preferences or identify the underlying causes of process inefficiencies and failures. Established businesses aim to monetise such knowledge, for example, to reduce costs, improve customer satisfaction, identify new product opportunities and increase sales. Similarly, societal benefit can be achieved by means of medical and scientific breakthroughs, etc. In addition, Big Data will enable new business models and create opportunities for innovative start-up companies.

In order to achieve the economic benefits of Big Data, a number of security issues need to be addressed, including the following:

- Clearly, the data security issues identified above in 7.1 also apply to Big Data. However, its volume, velocity and variety is likely to challenge the speed and scalability of some 'small data' solutions. For example, applying encryption at scale and speed is a major challenge.
- Big Data technologies and their implementations are likely to possess novel vulnerabilities that can be exploited by threat agents.
- A satisfactory balance needs to be found between the ability of individuals to control what is known about them and how it is used, and the legitimate aspiration of businesses to profit from new, improved and personalised/targeted services. The aggregation of data from disparate sources in hubs offering services to third parties is likely to complicate this issue by making the provenance of derived data difficult to trace.
- It is part of the *raison d'etre* of Big Data Analytics to enable the discovery of latent information. It is entirely possible, therefore, that commercially-sensitive or private and confidential information is exposed inadvertently in Big Data repositories. A well-known example of this is the re-identification of anonymised data. Techniques are available to guard against re-identification, but they inevitably also reduce the value of the data.
- A significant factor will be understanding where Big Data analysis will provide benefit, which kind of problems are likely to be amenable to the approach. There is also the degree to which Big Data can offer diagnostic insights and predictive capabilities, and how it can be combined with other techniques, for example agent-based techniques, so that it becomes more than a 'black-box' tool.

Big Data technology can also be applied to enhance security. For example, an enterprise may aggregate security-related logs in a central Data Lake and apply advanced analytics in real time to detect attacks at an early stage and trigger appropriate responses. Similarly, external information sources, including social media feeds, can be analysed to generate threat intelligence to warn a company of an impending denial of service attack by hacktivists, or a government agency of a potential terrorist attack.

Finally, the use of Big Data technology by threat actors themselves should not be ignored.

7.6. Internet of Things

The Internet of Things (IoT) connects physical objects, i.e. “things” embedded with electronics and sensors, to the Internet. These things are manifold, such as household appliances, traffic or car sensors, industrial Internet, health devices or smart meters. Due to the fact that these objects or things are mostly not designed under security aspects, new threats arise for the society at large. Besides the collection and linking of personal data by these objects, the interference of safety and security gets more important.

Therefore, since the Internet of Things involves a combination of different sub-systems whose safety goals may not be closely coordinated, it is important to be able to map, investigate and predict the interactions between these sub-systems in order to ensure the dependability of the global one. Existing approaches overlook the fact that the sub-systems in the IoT interact with each other in order to accomplish a common safety goal, and the fact that sub-systems with conflicting safety goals will still interact with each other.

Specific requirements will be:

- Find methods to ensure security in IoT at the device or component, network, and system levels and in its entirety,
- Define minimum international standards for networking and security of objects as well as dealing with the collected data,
- Take measures to ensure the responsible use of personal data collected at large by these active devices (sensors, cameras, smart meters etc.),
- Explore the dependencies of safety and security,
- Strengthen resilience and autonomy of objects, components, systems and infrastructure instead of perimeter security through better diagnosis, self-learning ability, and corrective adaptation to new circumstances.

In this context, the technologies used will need to employ measures that provide protection against attacks:

- Guarantee secure communication, since this will often occur via wireless communication interfaces. This will require technologies for ensuring that communication only takes place with authenticated and authorized partners. In addition, it will be necessary to guarantee the integrity and confidentiality of the data being transmitted. Data will need to be protected against interfering and eavesdropping.
- Guarantee the availability of communication. This is especially important when data need to be up-to-date and real-time requirements must be fulfilled. Moreover, when data that can be traced back to individuals are being processed, it will be necessary to employ technologies that protect the privacy of the Internet of Things users.
- Provide protection for the various systems, devices and components that form part of the Internet of Things, since these are often deployed in public places and are therefore highly susceptible to attacks involving physical alteration. Consequently, the data stored on these systems need to be protected against alterations, unauthorized access and destruction.

Security needs to be addressed not only during the development stage of the IoT but also once it is up and running. This will require engineering capabilities that enable implementation of security concepts for ensuring that the systems are both Secure by Design and Secure during Operation. Some approaches are:

- Attack prevention: encryption can be used to prevent eavesdropping as long as hackers do not have access to the relevant cryptographic keys. Meanwhile, attack detection technology can be used in situations where it is not possible to prevent attacks, as well as to assess the effectiveness of attack prevention technologies and to trigger appropriate responses. These technologies include Intrusion Detection Systems that detect suspicious behaviour by communication partners and attestation processes capable of instantly recognizing when a system has been tampered with.

- Recovery: technologies such as self-healing, as well as the ability to tolerate attacks up to a reasonable point.

Finally, the goal, wherever possible, is to prevent any threats to privacy or at least to keep them to the minimum possible and to make sure that any remaining threats are clearly identified. Usually, when a system is designed, its specific privacy requirements are taken from the relevant legislation for its area of application. However, since the Internet of Things constantly adapts to new requirements and cooperates with other systems, it is no longer possible to precisely define their area of application.

7.7. Securing Information in 'the Cloud'

Cloud computing is a business model that combines a multitude of technologies to provide remote, dynamic and flexible IT services. Since its emergence, there was a tendency to consider cloud computing security as the security of its technical components. However, as its initial years pass and the obstacles that prevented its proliferation are studied, it emerges that there are security considerations that are specific to cloud deployments.

Cloud computing signifies a transformation of the established ICT deployments for organizations and individuals: from an on-premise IT infrastructure to an off-premise IT service. The associated security controls and mechanisms are also migrating with the infrastructure: security is no longer in the hands of the user. What is lost in the process is the "sense of security and control of the user/IT manager", which is the most difficult to re-establish.

The above is mostly true for public clouds and hybrid clouds. Private clouds are exposed to similar threats as in-house ICT infrastructures and do not represent novel security challenges (except perhaps related to their size, which might make them attractive targets).

Specific requirements will be:

- Technology accessibility: Most public cloud services rely on proprietary implementations. Their data structures, middleware technologies and security mechanisms are guarded as trade secrets. As a result, efforts to make them more secure remain within the domain of the associated companies. However, these companies might not always feel compelled to make their systems more transparent and accessible to users and researchers. This provides a major challenge for cloud security research as well as interoperability, not mature yet, and compliance efforts. Incentives need to be created for these companies to move to more open structures and operation models as well as the promotion of open source alternatives. Scalability (for security, compliance, data retrieval and indexing) is also needed.

- Increased target vector: As many services and data are concentrated in cloud service provider data centres, these become very attractive targets for attackers. While experienced security personnel run these systems, it is still a challenge where

so many valuable assets and services are concentrated. Denial of Service attacks and disaster recovery become even more significant under these circumstances.

- Insider threats: As almost total control of data and applications and infrastructure is transferred to cloud service providers, insider threats within these providers become a major concern.

- Cloud Model Selection: Most companies and individuals might prefer to move to a public cloud to minimize their costs and might prefer SaaS as the least technologically demanding solution. However, a proper risk assessment needs to be carried out on the assets and targets of each company, and a proper model needs to be selected based on the threats and risks identified. A hybrid or community cloud might be less risky for some organizations. As long as organizations do not make this assessment in cloud service and model selection they place themselves and their dependents under major risks. Proper risk assessment tools need to be provided for this purpose.

- Trust erosion: The biggest challenge for the current clouds, however, is concerning to methods to establish presumptive trust on an evidence base, and to nurture the initially established trust relationship into one of trustworthiness in order to facilitate social and economic transactions. In dynamic systems and applications, such as in cloud computing, the sole expression of access rights is not enough. Policies for dynamic systems usually allow data providers to express which attributes may or may not be collected, but we need to allow data providers to specify provisions and obligations.

- Privacy: Privacy challenges in future cloud computing are related to the need to protect data on-premise and in-transit and ensure access to it by authorized parties only, including transaction histories for potential privacy-enhancing user tools as well as for compliance and forensic purposes.

- Software and hardware architecture used by cloud providers: Current cloud computing relies on virtualization technologies to isolate client data and applications, which carry new technical controls with implications on privacy and security. Providers also rely on client-side, perimeter, and web browser security. It is important to understand all the technologies used by cloud providers for their services. This translates into an expanded attack surface and, consequently, new risks and threats. Just recently new vulnerabilities have been found in virtualization solutions, which gives an idea of the challenges with respect to the underlying architecture used in cloud offerings.

- Authorization and Authentication: data protection, federated identity management issues.

- IT-forensic in clouds: increasingly data is stored in decentralized locations, e.g. using cloud locations or even cloud services. This is also the case for stolen or illegally copied data. Data stored in clouds shall have the same level of protection as usually stored data. Nevertheless during investigations e.g. performed by LEA, it is difficult to distinguish and separate between illegal and legal data, missing harmonized cross-border (European wide) regulations impede the work of LEA or will conflict the need for data protection. Challenges are in the technological and legislation/regulation area.

7.8. Technologies applied to Cybersecurity

Adaptive Cybersecurity technologies are necessary to address the 'moving target' nature of cyber threats. Such technologies need to be flexible, agile and responsive, enabling

them to cope with the future network bandwidth and be more successful against zero-day attacks.

Adaptive techniques will produce some of the most effective methods of threat detection/prevention. In fact, some threats such as Insider Threat and Identity Masquerading will potentially only be caught by using adaptive techniques. Adaptive techniques will also introduce opportunity for efficiency in terms of minimising the cost of security where, depending on a given scenario and resources available, the most effective mix of techniques can be utilised for the most efficient result. Adaptive techniques can also provide simplified and efficient reports to users and operators.

Humanity adapts and changes constantly and systems need to be able to recognise and deal with an adapting society. Systems view should be taken, considering People, how they generate Data, which feed Applications, running on Devices connecting to the Cloud and Internet.

On the other hand there are also some risks from using adaptive technologies and aspiring to have autonomous systems. Adaptive techniques could introduce new vulnerabilities. There is a risk of systems learning the wrong thing and Swarm Technologies and Herd Mentality theory was highlighted. Key to a research roadmap is having access to and demonstrating solutions on real-world data. Applied researchers need to work with government and industry partners to realise this, connect with the various cyber ranges and aspire to have a standard dataset within the community.

Specific requirements will be:

- Normalising/Protecting Systems. Systems need to be able to measure within a closed loop; however the potential dangers of in-band control signalling were highlighted. Adaptive security technologies need to carry out behavioural analytics and behavioural- based trust. In doing so, security mechanisms should be designed to
    - minimise interference with normal operation
    - control the degradation of systems performance and
    - maintain a minimum Quality of Service.

- In normalising / protecting systems researchers should look at what can be learned from safety critical systems and their approach to architectures and systems engineering. In decomposing complicated intelligent behaviour, researchers should look at Brooks' work on robotics and subsumption architectures.
- Hi-Fidelity Detection. Adaptive systems are needed to reduce false positives and false negatives in current detection techniques. Researchers should use big data to their advantage, separate the data from the system, isolate what can change and what is static, and carry out content level analysis. Researchers should look to apply adaptive Cybersecurity technologies to reduce the cognitive burden on humans and harness nature- inspired mechanisms that can deliver faster-than-human response.
- Intelligence Gathering/Learning/ Information Sharing. Adaptive systems will need to be cognitive and have some level of self- awareness, self-learning and self-explanation to be able to address a moving target. There will need to be some predictability based on past data that essentially allows the database to be able to reason about the future, run 'what if scenarios' and learn from wrong decisions. Adaptive systems will need to be able to verify, prove, explain and justify system actions. Researchers should look to employ out-of-band management communications, look at new techniques of visualisation, and develop systems that can not only self-learn but will contribute to and learn from the community. Autonomous systems should be developed that automatically learn from attacks and

share this learning to a network for all. In turn, this open source information will allow the autonomous systems to profile and mitigate potential attackers and deliver early warnings of hostile reconnaissance.

- Adaptive systems need to be cognitive to address a moving target and be able to verify, prove, explain and justify system actions. Systems need to self-learn and be able contribute to and learn from the community.
- The development of Cybersecurity technologies which have:
    - self-learning capabilities;
    - self-awareness in cyber systems enabling early attack detection and self-configuration to defend against an attack;
    - the establishment of feedback in cyber systems providing the capability of learning from cyber attacks.
- Safety critical systems and subsumption architectures in robotics.
- To be able to normalise and protect systems, it is needed to look at systems engineering approaches of safety critical systems and subsumption architectures in robotics.
- Adaptive techniques that use Big Data to their advantage and harness nature inspired mechanisms to deliver faster response and provide Hi- Fidelity detection.
- Cyber-physical protection systems. The research activity encompasses the whole cycle of electronic access (including authentication and authorization/profiling of users), network control, and system monitoring with respect to complex, distributed ICT systems. Users can be individuals, groups, physical objects, logical entities, or applications. The objective is to make the interconnected system of national critical networks and individual infrastructures more resilient and secure. This is typically achieved by a combination of means, and in particular: i) enforcing both passive (firewalls) and active (intrusion detection and prevention) perimeter defence systems, ii) improving the technologies for design and development of network protocols and services, and iii) continuously monitoring network status and traffic. Network protection is of paramount importance, since it is a pillar on which many other vital aspects of the modern society are based. With respect to prevention and investigation, lawful interception is a key topic. Important mechanisms also include intrinsic security of unmanned systems, and specific solutions for secure network communication in wireless segments (e.g. surveillance, intrusion detection, and mitigation of cyber attacks). More effective convergence is needed among a plethora of Cybersecurity technologies, including: Physical Security Information Management (PSIM), Security information and event management (SIEM), Security Operation Centre (SOC), Identity Management, Building Automation, Video Surveillance, Access Control, and Forensics.
- Cyber intelligence via information management. The objective of the research activity is the development of effective cyber intelligence features, to guarantee citizens' global security, by exploiting the huge potential of currently available as well as emerging Information Management technologies (including high-performance and cloud computing platforms). Security will be improved along several axes, including protection of ICT systems, Critical Infrastructures, and assets. The developed technologies will provide a set of tools that will support a security process consisting of the following three phases: plan, control, and react. A key role will be played by information flow collection technologies, e.g. those based on video surveillance.

7.9. Cryptography

Cryptography underpins much of the digital infrastructure, and although it is a mature technology, the need to provide efficient cryptographic coding that is robust against rising computing power will always drive research. Much of this research is already well funded through programmes within Member States, so the H2020 programme should explore avenues that transcend national programmes or which look at radical new techniques or applications. For example, cryptographic techniques for micro-entities in the internet of things may have objectives and technological underpinning that will be significantly different from the established solutions.

8. CONCLUSION

This Secure Societies Strategy captures the perspectives of the members of the Advisory Group. This draws from a broad range of backgrounds and experience and is offered as a basis for developing the subsequent phases of the Horizon 2020 programme.

The Strategy focuses on areas where future emphasis should lie, recognising that much research and innovation activity has already been undertaken in FP7 and in the programmes of Member States.

The Advisory Group deliberately looked for shifts likely to take dominance in the 2020s, paying attention to the current day priorities but taking a longer perspective. This has led to some debate within the Advisory Group, and this document has tried to respect high priority short-term topics where there has been strong support from external groups.

A key element of this strategy is the approach outlined in Section 3, the development of Innovation Roadmaps.

This is seen as a means to develop the necessary integration and implementation detail that will enable H2020 projects to deliver high value outcomes, with a focus on engaging user organisations and fostering innovative demand from these use organisations.