**SECURE SOCIETIES**

*Protecting freedom and security of Europe and its citizens*

# STRATEGIC INPUT FOR 2016-2017 WORK PROGRAMME

**Produced by the Secure Societies Advisory Group**
**July 2014**

## INTRODUCTION

The Secure Societies Advisory Group (SSAG) has considered the strategic priorities that should shape the H2020 programme for the 2016/2017 Call by the following process:

- The inaugural meeting identified 'close-to-market' aspects of innovation as of especial significance to this theme, and also the need to be able to respond to rapidly developing threats through a fast track process. Sub-groups of the SSAG developed working papers on both these aspects.

- The second meeting addressed the principle challenges being faced, and identified the following areas where strategic focus was required:

  1. The systemic issue of p**lanning and integrating advances** across technical areas or missions, meeting user needs in a directed way to generate a market, complementing bottom-up capability and critical technology research. This has stimulated a proposal for a mechanism that provides resources to manage the production and maintenance of roadmaps including results monitoring and gap assessment to capture and articulate how multi-disciplinary innovation reaches the market.

  2. **Social Dimension of Security**. The key assumption is that members of society are a collective player/stakeholder in the field of *security*. Society members are: users of the security research and development outputs; and can also be considered the end-users of the solutions in a less classical way—namely as beneficiaries of the results. In addition, 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 the direct customers of the *security* products and innovative solutions.

  3. **Crime and 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.

  4. **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 the normal definition of ICT to include infrastructure 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.

  5. **Cross-Cutting Capabilities and Issues**. The nature of the Secure Societies challenge theme makes it fundamentally dependent on cross-cutting links across the H2020 programme. Projects will often provide routes to market for emerging technologies. Strong approaches are needed to ensure H2020 projects can follow exploit advances across the Themes and from basic research, in the Key Enabling Technologies programme, and national fundamental research activities.

These areas have been developed by working groups of the members, the results of which appear as the Chapters that follow.

In addition, the SSAG recognizes that there are important areas that fall beyond the areas described above but which will need to be recognised in detailed work developing topics. These are areas that received considerable funding and support in FP7, and for this reason were given less weight for this Call, but it will be important in the topics development work running in the second half of 2014 to look carefully at FP7 projects underway and ensure that gaps and new developments are properly addressed. The areas that the SSAG has noted in this regard include:

- CBRNe.
- Maritime Security
- Critical Infrastructure Vulnerabilities, including safety design norms.

The document includes as Appendices two working papers addressing our overall Strategic Vision and our proposals for Fast Track Innovation.

## CHAPTER 1:
## PROPOSAL TO PROVIDE INNOVATION ROADMAPPING AND COORDINATION SUPPORT TO HIGH PRIOIRTY SECURITY OBJECTIVES

### 1. Summary

This proposal originates from the Secure Societies Advisory Group and addresses the need to develop and monitor the *innovation architecture*[1] in topic areas that depend upon

- integration of advances across a number 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 outcome that would develop and maintain, amongst other things, a technology roadmap linking advances in specific capabilities to particular market needs. We are calling this 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.

We consider this needs to be an appropriately resourced activity that would involve stakeholders from academia, industry, 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 we see a special type of Coordination and Support Actions (CSA) being most appropriate. 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.

### 2. Rationale

The Secure Societies advisory Group recognised a number of issues arising from experience in FP7 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:

a. <u>User engagement.</u> 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 and user processes and behaviours. Getting significant user engagement in R&I has been a challenge, in part because of time pressures on users and also the lack of a framework for their input to be harvested efficiently.

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

[1] 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.

c. Limited deployment of integrated solutions. Achieving deployable outcomes usually requires integration of several advances across capabilities, rather than a single linear project. Beyond the larger demonstrator projects, FP7 had limited support to enable teams in complementary projects to map out how an integrated solution would be achieved, leaving an unbridgeable gap between fragmented project outcomes and deployable solutions that users could recognise and embrace.

d. Vague routes to market. The route to market for successful topics was often unclear. In a commercial market the payback from investing in research can be assessed in terms of market research and understanding that businesses build internally. In the security area the market is largely determined by procurement plans and policies in public sector organisations. Accepting security markets will always have uncertainties, more can be done to identify potential early adopters, procurers and their timelines.

e. High bid costs. Bidding costs are high and bid teams have to make assumptions about the wider context of their proposals. Greater visibility of the wider innovation landscape in an innovation area would simplify bidding and lead to better targeted projects.

f. 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 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:

> The security market has three distinctive features:
>
> *(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 approach to linking fundamental technology, solution creation and market pull to accelerate innovation that targets priority outcomes and stimulates effective 'innovation chains'.

## 3. The Proposal

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 can also address 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:

a. What are the main requirements and opportunities in an area?

b. What are the driving trends?

c. How does research map to produce solutions that meet user needs (currently stated and latent) and in what procurement timescales or windows of opportunity exist.

d. Are there potential solutions that early adopters would embrace?

e. What gaps exist in the current research landscape, and what are the priorities in the short, medium and long term.

f. What linkages are relevant to other parts of the H2020 programme?

g. 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, people 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 cold 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.

The outputs of the Roadmapping CSAs would be:

a. Description of the field and partners,

b. A suitable form of roadmap[2] that shows how different capabilities integrate to produce solutions, and how these solutions are expected to be taken up by users.

c. Proposing candidate areas for R&I activity for future H2020 calls, Programming or cluster approach as mentioned in the SAG Strategic Vision.

d. 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.

e. A regular review of progress in projects relevant to its field of interest.

f. Indications of where early adopter interest should be stimulated to bring solutions more rapidly to deployment.

g. Repository of knowledge and experience, support for a vibrant innovation community.

## 4. Establishing the Innovation Roadmapping CSAs

The Secure Societies Advisory Group would recommend areas where CSAs could be beneficial, and it is expected that the Commission, responding to the priorities of the Programme Committee, would identify IRCSAs for the 2016/17 Call, leading to competitive responses by bidders proposing to undertake the action. The CSAs would therefore commence in 2017 and play their full part in informing the 2018 Call. In the meantime, the Secure Societies Advisory Group would undertake some of the functions through informal means such as workshops.

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. We note that 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’ and Disaster resilient Societies themes could be candidates:

- Advanced easy to use forensic tools + Internet forensics to combat organised crime
- Securing vehicle supply chains from production to destruction
- All the Urban Security topics
- All the Ethical/Societal Dimension Topics
- CBRNe (Chemical, biological, radiological, Radiological and Nuclear, explosives) in all phases from preparedness to long term recovery.

[2] 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.

## CHAPTER 2
## SOCIAL DIMENSION OF SECURITY
### *Security and trust of the citizen*

QUESTION 1: WHAT IS THE BIGGEST CHALLENGE IN THE FIELD CONCERNED WHICH REQUIRES IMMEDIATE ACTION UNDER THE NEXT WORK PROGRAMME?

From a societal perspective, perception of *security* cover a number of aspects:

A. The objective security of members of society
B. Beliefs about the security of oneself and others
C. Subjective security in particular contexts and circumstances
D. Perceptions of the value and appropriateness of security measures

The strategy of the future *security* research within the **SOCIAL DIMENSION OF SECURITY** theme can be built on a twofold understanding and approach:

a) **the short-term** strategic research challenges

b) **the long-term** 'closer to market' innovation challenges

**The short-term** strategic research 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 and 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).

The key issues to be addressed within include:

(i) differences in national and local perceptions of *security*;
(ii) differences in approaches to *security* amongst different stakeholders;
(iii) the need for citizens to be aware of *security* risks and protect themselves, without feeling afraid unnecessarily;
(iv) the role of emotions and values in feelings and perceptions of *security*;
(v) the need for policy makers to understand and respond to citizens' concerns, but not be driven by beliefs that may be misguided and
(vi) the role that media play in creating the common perception and understanding of *security*.

There is a need to better understand and evaluate the societal impact of *security* measures—this would be beneficial for all stakeholder groups; and (vi) 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.). Also the social trends (e.g. social media) shall be examined 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.

**The long-term** 'closer to market' innovation challenge would be to respond to the needs and expectations of the society taking into account that today's world is getting more and more *personalised* in terms 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 is an active player in the field and the beneficiary as well as 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: 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, 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.

## QUESTION 2: WHAT ARE THE KEY ASSUMPTIONS UNDERPINNING THE DEVELOPMENT OF THESE AREAS (RESEARCH & INNOVATION, DEMAND SIDE AND CONSUMER BEHAVIOUR, CITIZENS' AND CIVIL SOCIETY'S CONCERNS AND EXPECTATIONS)?

This area is fully dedicated to the citizen and society concerns and expectations.

The basic assumption for that area is that members of society are a collective player/stakeholder in the field of *security*.

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 a less classical 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 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, RTOs and policy makers, in order to achieve the common understanding of the needs and requirements for *security* research and its products.

Those assumptions are based on some available results of the previous foresight studies, including FP7 projects such as e.g. ForeSec, Focus or Festos.

### QUESTION 3: WHAT IS THE OUTPUT THAT COULD BE FORESEEN, WHAT COULD THE IMPACT BE, WHAT WOULD SUCCESS LOOK LIKE, AND WHAT ARE THE OPPORTUNITIES FOR INTERNATIONAL LINKAGES?

The desired output of the research actions would be to achieve a common understanding of the *security* within the different group of stakeholders and to strengthen the mutual trust of the society and governing authorities. The expected impact shall cover also levelling the differences in understanding and sense of *security* between citizens of different countries. The success would be to create within the EU society a *security* aware community of EU citizens able to actively participate in the *security* processes. In terms of technology – new innovative products designed for personal use or new ways of using the existing solutions and processes will be the goal.

### QUESTION 4: WHICH ARE THE BOTTLENECKS IN ADDRESSING THESE AREAS, AND WHAT ARE THE INHERENT RISKS AND UNCERTAINTIES, AND HOW COULD THESE BE ADDRESSED?

The bottlenecks in this case can be summarised in one that is the “human factor”. The way of finding balance between what is considered an individual vs. collective value, ways and means of communication, individual characteristics and preferences, which are hard to measure and describe. Methodologies and tools for the sociological/foresight research shall be revised to be less academic towards a more application oriented approach.

### QUESTION 5: WHICH GAPS (SCIENCE AND TECHNOLOGY, MARKETS, POLICY) AND POTENTIAL GAME CHANGERS, INCLUDING THE ROLE OF THE PUBLIC SECTOR IN ACCELERATING CHANGES, NEED TO BE TAKEN INTO ACCOUNT?

Research into feelings of security has focused on the urban environment—mainly on safety in public places after dark. However, little is known about feelings of *security* in relation to cybercrime, border control, large events. It may be problematic to consider feelings and perceptions of *security* in relation to all types of crime, terrorism, cybercrime, and disasters. We also know that quantitative surveys have serious design flaws, and that the results may be misleading. Quantitative surveys aimed at citizens may be particularly problematic when applied to rare events such as disasters or terrorism.

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

## QUESTION 6: IN WHICH AREAS IS THE STRONGEST POTENTIAL TO LEVERAGE THE EU KNOWLEDGE BASE FOR INNOVATION AND, IN PARTICULAR, ENSURE THE PARTICIPATION OF INDUSTRY AND SMES? WHAT IS THE BEST BALANCE BETWEEN BOTTOM-UP ACTIVITIES AND SUPPORT TO KEY INDUSTRIAL ROADMAPS?

Some areas, by essence inter-disciplinary, have been initially identified as requiring addressing:

**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).

**Immigration** – improving security, without promoting segregation, racial prejudice, social exclusion, etc.; security, social inclusion and wellbeing.

**Social control** – large events; large residential buildings; public/accessible facilities containing ICT; urban transport (e.g. trains, light rail).

**Trust** – communicating with citizens about security, without undermining trust; fostering social support within urban environments to help improve feelings of security.

**New emerging risks** – designing for security, potential dangers of technologies considered from the outset; addressing crime prevention within the early stages of the product development process; the costs and benefits.

**Mass threats with high social impact** (CBRNe, natural and industrial disasters, terrorism[*]) – preparedness and response, early stage prevention and aftermath management, education and training, double use technologies.

[*] *Understood as acts of single individuals not organised groups (blowback attacks by foreign fighters coming from modern wars; Breivik-like attacks etc.)*

## CHAPTER 3
## CRIME AND CRIME PREVENTION
***The search for new methods and tools to sustain future crime challenges***

This document has been prepared by a working group of 5 members who span a spectrum of expertise in the crime related disciplines", meanly end users from law enforcement. We have adopted the title of "Crime and crime prevention" to capture our view that there are a range of 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.

Crime and crime prevention is inter-connected with the other responses of the SAG, but due to its origin currently not always technology related. This response will need an integrated approach connecting policies, society and technology to strengthen and protect the society as well on European, National, regional and individual level.

### QUESTION 1: WHAT IS THE BIGGEST CHALLENGE REQUIRING IMMEDIATE ACTION?

The biggest challenge 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 society disruptive crimes. The "new generation of crimes" is 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.

The fast and new appearance of new generation crimes or the use of old crimes in new geographical zones looks to be undetectable, unsolvable with perpetrators who are unanimous or not red handed caught.

### QUESTION 2: WHAT ARE THE KEY ASSUMPTIONS UNDERPINNING THE DEVELOPMENT OF THESE AREAS (RESEARCH & INNOVATION, DEMAND SIDE AND CONSUMER BEHAVIOUR, CITIZENS' AND CIVIL SOCIETY'S CONCERNS AND EXPECTATIONS)?

European boundaries are fading: physically, culturally and virtually. Due to the speed of evolution, an irreversible cause and uncontrollable effects, national responsible bodies and civilians are confronted with crime and its effects that need inter Member State alliance and methods. The methods need to provide the Member States with a new level of understanding, forecasting new trends, recognizing current trends and quick joint and lean responses.

Of course, one of the boundless appearances of crimes is spread through the Internet, causing cybercrime in all its ways of appearance. This is seen as an emerging spreading phenomenon. To protect civilians and economy, this needs a compendium of methods preventing and fighting crime.

The other new appearance is caused by not forecasted, not foreseen crime related to the auxiliary structure of a free Europe, enabling the free transport of people and goods. This can be seen as a cross cutting new challenge where for instance DG Home, DG Move, DG Regio, DG Market, DG OLAF could be partners to be aligned but also the Member States. Member states will be 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.

Although we have a European Union with policies in place, a fast response in this area is appropriate activating operational actions.

## QUESTION 3: WHAT IS THE OUTPUT THAT COULD BE FORESEEN, WHAT COULD THE IMPACT BE, WHAT WOULD SUCCESS LOOK LIKE, AND WHAT ARE THE OPPORTUNITIES FOR INTERNATIONAL LINKAGES?

Main outputs should be:

- Forecast and understanding of fast appearing or potential new crimes,
- Delivery of new methods, implementable for crime reduction and prevention,
- Improvement of information sharing, not only through a better connection of Member States information management systems but also through new methods of recognizing crime trends and prevention methods through other sources,
- Enhancement of the interoperability between Member States, based on legislative agreements and fast track innovative solutions for law enforcement,
- A better usage of technology and science in crime fighting and prevention.

## QUESTION 4: WHAT ARE THE BOTTLENECKS, RISKS AND UNCERTAINTIES AND HOW COULD THESE BE ADDRESSED?

Traditional ways of crime fighting and prevention are implemented and their 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. Crime and crime prevention will need flex and fast measures and resources causing justly discussions on competence and ethical rules.
Relate to "real case scenarios", recognisable for European and National Policymakers, but above all to the leaders of law enforcement and who are responsible, is needed.

In Cybercrime this is already a "lesson learned": although the impact and potential of Cybercrime was detected (after noticing that it is irreversible), supporting structures are understaffed and there is no EU alliance.
In the domain of new other crimes, this can be even a more prominent case.

Uncertainty is caused by the difficulty of impact and output measuring whenever new methods will prevent an unidentified number of prevented cases.

Bottleneck can be the wish to register and sense the current state of play in crime, wanting to know the right point of departure and the wish to monitor the progress and exact outcome. Due to the fast changing appearance of crime, its adaptability on counter measures, this needs a new innovative approach where fails are seen as lessons learned and the exact effect may be an assumption.

## QUESTION 5: WHICH GAPS AND GAME CHANGERS NEED TO BE TAKEN INTO ACCOUNT?

There is a potential gap in knowledge related to crime. Citizens most often do not declare crime unless they suffer financial costs that need to be reimbursed by the insurance companies. Whenever crime is related to serious and organized crime, only directly severe impact (e.g bank robbery) will be registered. "Smart" serious and organized crime will be unrecognisable, unforeseen but will mostly have the highest indirect impact on security. Examples can be found in the logistic sector, smart drugs, financial markets, brand forgery and in the Cyber space.

Game changers can be new innovations that will unintentionally cause new crimes. The latest trends in 3D printing proved that producing of a gun just needs a very low cost 3D printer.

Another gap could be the technology providers unsure if this market is profitable due to sometimes small scale and very evolutive solutions and market. Next to sensing and communications systems, new innovation is needed enabling also unforeseen (parallel) markets for security technology.

## QUESTION 6: IN WHICH AREAS IS THE STRONGEST POTENTIAL TO LEVERAGE THE EU KNOWLEDGE BASE FOR INNOVATION AND, IN PARTICULAR, ENSURE THE PARTICIPATION OF INDUSTRY AND SMES? WHAT IS THE BEST BALANCE BETWEEN BOTTOM-UP ACTIVITIES AND SUPPORT TO KEY INDUSTRIAL ROADMAPS?

The mostly technology driven road mapping from the industry and SMEs could be used to see how these roadmaps could be made suitable for security as above mentioned (technology push).
Road mapping from the challenge and business crime side demand will discover new applications for technology (technology pull based on societal studies).
The best balance should be achieved by integrating approaches for society means including the societal science and industrial road mapping.

This approach will activate Research and Innovation Actions as well joint procurement.

Some Key enabling technologies are listed below:

- Technologies that can anticipate sufficiently in advance the 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 suing these technologies is to discover what are 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.
- 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.
- Technologies and social sciences methods (approaches) that help understanding how organised crime exploits socio-economic conditions for the crime actors benefit.
- Technologies for monitoring developments-based, well targeted, indicators for extracting relevant information for analysis coming from a variety of sources. This is crucial for understanding the criminal strategies and anticipating their trends and actions.
- Enhanced forensic methodologies and tools
- Enhanced technologies for surveillance (CCAT) and image processing, fast and reliable identification of objects…

## QUESTION 7: WHICH AREAS HAVE THE MOST POTENTIAL TO SUPPORT INTEGRATED ACTIVITIES, IN PARTICULAR ACROSS THE SOCIETAL CHALLENGES AND APPLYING KEY ENABLING TECHNOLOGIES IN THE SOCIETAL CHALLENGES AND VICE VERSA; AND CROSS-CUTTING ACTIVITIES SUCH AS SOCIAL SCIENCES AND HUMANITIES, RESPONSIBLE RESEARCH AND INNOVATION INCLUDING GENDER ASPECTS, AND CLIMATE AND SUSTAINABLE DEVELOPMENT? WHICH TYPES OF INTERDISCIPLINARY ACTIVITIES WILL BE SUPPORTED?”

Integrated activities are foreseen at:
- Member State level,
- European (DG) policy level,
- SME’s and industrial actions to integrate new technology.

Furthermore this topic will intersect with strategic agenda’s and development as Smart cities, ICT developments (Avatars), sensor development and implementation of societal studies in technology (recognizing patterns predicting crime, crime area’s)…

## CHAPTER 4
## "DATA2020"
## *Data Protection, Resilience and Privacy*

This document has been prepared by a working group of 10 members who span a spectrum of expertise in the cyber related disciplines. We have adopted the title of "DATA 2020" to capture our view that there are a range of issues relating to the use and protection of data that are difficult to separate, with many trade offs implied, and that the key challenge is how to reconcile these issues in a practical, ethical and legal way.

We assume that the specific technical aspects of the subject will be led by the inputs under DG Connect, so our input emphasises the interplay between technical and societal/business dimensions, but recognising that there is a broad overlap to be resolved at a later stage.

### QUESTION 1: WHAT IS THE BIGGEST CHALLENGE IN THE FIELD CONCERNED WHICH REQUIRES IMMEDIATE ACTION UNDER THE NEXT WORK PROGRAMME? WHICH RELATED INNOVATION ASPECTS COULD REACH MARKET DEPLOYMENT WITHIN 5-7 YEARS?

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, 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.

These challenges overlap other areas of H2020 activity and this poses a difficult problem in giving a response to this question that is meaningful and focussed. The SSAG took the view that the focus should be on three aspects:

- **Data Protection**, taken to 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.
- **Resilience of Data.** 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.
- **Privacy**, taken to include 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.

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.

Aspects Addressing Data Protection

- Repeated compromise of personal data has resulted from failure to implement best practice in the holding of this data, suggesting the need for stronger information governance in organisations, technical control, and possible greater regulation, with norms on compensation and redress.
- 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.
- The “shielding principle” (build a fortress) does not work anymore (e.g. firewalls, secure networks, secure routers). Security of services and data must be facilitated assuming wider sharing and access to data, including across even insecure systems, networks and services. Protection needs to be at the data level as well as across systems.
- 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.
- Cyber security related practice oriented information, composed with forecasting information build a central building block to ensure appropriate and adequate reaction and prevention.
- 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.

- 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.

Aspects Addressing Resilience

- 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.
- 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.

Aspects Addressing Privacy

- Innovation: 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.
- Privacy challenges: 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.
- Exploitation of Big Data shows an exponential rise, yet privacy arrangements in social media and other public repositories are fragmented and largely immature.

- 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.
- Fast surveillance of person on distance: development and integration of next generation technologies and solutions for fast detection (screen while walk detection in a flow) of threats (e.g. of explosives/dangerous (hazardous) goods and materials / weapons / pyrotechnics without conflicting privacy
- 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

## QUESTION 2: WHAT ARE THE KEY ASSUMPTIONS UNDERPINNING THE DEVELOPMENT OF THESE AREAS (RESEARCH & INNOVATION, DEMAND SIDE AND CONSUMER BEHAVIOUR, CITIZENS' AND CIVIL SOCIETY'S CONCERNS AND EXPECTATIONS)?

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 the 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 & privacy management, means to raise awareness and public engagement, etc..

Two 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”.

## QUESTION 3: WHAT IS THE OUTPUT THAT COULD BE FORESEEN, WHAT COULD THE IMPACT BE, WHAT WOULD SUCCESS LOOK LIKE AND WHAT ARE THE OPPORTUNITIES FOR INTERNATIONAL LINKAGES?

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 that address the issues highlighted under Question 1,
- Guidance and regulations that strengthen information governance in 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, they do not perform in the same for all users, but which can still be shown to comply with 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 (i.e. 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 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.

## QUESTION 4: WHICH ARE THE BOTTLENECKS IN ADDRESSING THESE AREAS, AND WHAT ARE THE INHERENT RISKS AND UNCERTAINTIES, AND HOW COULD THESE BE ADDRESSED?

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.

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 Cybersecurity is the fact that many risks arise because of determined malicious malefactors able to exploit gaps in capability opportunistically. 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 where proposed that can "learn" itself 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.

## QUESTION 5: WHICH GAPS (SCIENCE AND TECHNOLOGY, MARKETS, POLICY) AND POTENTIAL GAME CHANGERS, INCLUDING THE ROLE OF THE PUBLIC SECTOR IN ACCELERATING CHANGES, NEED TO BE TAKEN INTO ACCOUNT?

There are significant technological gaps, for example in how to strengthen end-to-end security or support strong identity authentication. But there are also a significant range of issues that are under the heading of *information governance* that need development, for example regulatory and legal aspects of holding personal data. Potential game changers could include:

- 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,
- Massive data processing through cloud computing and Big Data are two game changers that authorities should keep regulated. These regulations should be agreed internationally, as attackers/criminals can be from any country,
- The most challenging issues with origin in the technological changes lay in the 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,
- Enhanced biometrical authentication methods that are easy to use but also revocable might reduce need for various existing methods,
- Also 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.

## QUESTION 6: IN WHICH AREAS IS THE STRONGEST POTENTIAL TO LEVERAGE THE EU KNOWLEDGE BASE FOR INNOVATION AND, IN PARTICULAR, ENSURE THE PARTICIPATION OF INDUSTRY AND SMES? WHAT IS THE BEST BALANCE BETWEEN BOTTOM-UP ACTIVITIES AND SUPPORT TO KEY INDUSTRIAL ROADMAPS?

The issues covered here are fundamentally of a global and cross-Europe nature, 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.

This means the Secure Societies programme in H2020 must stimulate research and innovation that can deliver high impact and support Europe as a leader in appropriate areas of this subject. This implies a strategic approach based on top-down and bottom-up road maps that can link together advances in technology and human sciences with objectives targeted at citizens' needs and business's priorities.

Part of this should be the creation of an ecosystem dedicated to security & privacy. This might take integrate solutions, products or services providers associated with certification and controls in a context of regulations creating the market. Actors will be of various profiles opening the market to various company types (inc SMEs). It has to be noticed that in some areas the ecosystems exist, and where Europe has the leadership (smartcards, secure integrated circuits, etc.).

The areas in which the EU innovation could bring more benefits to the citizens is in safeguarding their cyber security and privacy and in making them knowledgeable of the measures taken for this, in order to increase their trust. Empowering the role of the Technological centres as EU knowledge transfers can catalyse the innovation in Europe, especially by providing training, tools, assistance, etc. to SMEs.

One problem seems to be the temporal gap between research and innovation and having a product to sell, especially for SMEs. Therefore it is important to include in European projects not only the research units of industry, but to also their business units to ensure understanding of the return on investment is well founded.

Security solutions driven by industry often do not take into account end users' and data owners' perspective. The EU can then have a primary role fostering development of solutions that provide actual protection and control for users and data owners. This will strengthen EU leadership and provide competitive advantage to European companies developing technologies to support these requirements

## QUESTION 7: WHICH AREAS HAVE THE MOST POTENTIAL TO SUPPORT INTEGRATED ACTIVITIES, IN PARTICULAR ACROSS THE SOCIETAL CHALLENGES AND APPLYING KEY ENABLING TECHNOLOGIES IN THE SOCIETAL CHALLENGES AND VICE VERSA; AND CROSS-CUTTING ACTIVITIES SUCH AS SOCIAL SCIENCES AND HUMANITIES, RESPONSIBLE RESEARCH AND INNOVATION INCLUDING GENDER ASPECTS, AND CLIMATE AND SUSTAINABLE DEVELOPMENT? WHICH TYPES OF INTERDISCIPLINARY ACTIVITIES WILL BE SUPPORTED?"

The domain of this field is inherently concerned with integrating technologies with social sciences and humanities to meet societal challenges. The area has obvious connection to underpinning ICT technologies, especially in areas of authentication, encryption, data loss prevention, Internet resilience, developments in personal ICT devices, embedded ICT in objects, location technologies, quantum electronics, developments in social media of all types. It is also closely related to developments in techniques used by malicious players.

Progress in this area depends upon effective means to bring complementary capabilities and expertise together, and to do this in a way that respects the different cultural and ethical outlooks across member states. Public Private Partnerships will play a very important role here, as it is extremely important to have governments, the private sector, and civil society engaging on these important issues for information sharing and building trust. It is expected that the issue cannot only be tackled at a technological level, but needs a much better understanding of societal consequences that arise from Big Data and the likely disappearance of privacy. Consequently, an open discussion that also touches upon novel governance and policy structures for a highly engineered future world has to be fostered.

Privacy, security and trust on internet applications are the areas in which the multi-disciplinary research can bring biggest success as they are in the interleave of social and technical knowledge: usability vs. performance, user security needs eliciting and understanding, user privacy options profiling, friendly notifications to user on incidents, etc. This applies also to cloud-based critical services and any other internet-based systems.

This domain is specific due to the crossing of several fields (economics, societal challenges, technology, psychology, law and classical crime prevention and investigation methods (forensic)). All these should be considered when launching supporting activities. This should be implemented in the future calls.

There are specific opportunities for integrated activity with the Key Enabling Technologies programme, and with the ICT element of the Industrial Leadership Pillar.

Key References

“Cybersecurity Strategy of the European Union” – 7th February 2013

## CHAPTER 5
## CROSS-CUTTING INNOVATION

The nature of the Secure Societies challenge theme makes it fundamentally dependent on cross-cutting links across the H2020 programme. Projects will often develop and stimulate routes to market for emerging technologies. Many of these linkages will only become clear once project teams put together and execute their detailed plans, and we can therefore rely on this bottom-up activity to forge many of the necessary co-dependencies.

However, there are linkages where research and innovation in the Secure Societies area will benefit from a strategic look at cross-cutting issues. These include:

- Communication technologies, including core developments in the internet, cyber security, authentication, mobile broadband, location and short range networks.
- Sensor technologies, including video, biometrics, photonics and chemical sensing, especially developments that make these low cost and field deployable.
- Climate change and availability of resources, including food.
- Health and all aspects of the human behaviour, including understanding how to better integrate people into complex systems.
- Advanced materials, including nanotechnologies, graphene,
- Robotics including UAVs

These potential linkages suggest possibilities for joint actions, or some form of strategic oversight across the relevant H2020 areas. As important will be to ensure that the results from resulting projects are promulgated effectively.

Mechanisms are needed to enable ‘solutioneering’ to take place across EU and national research programmes. This should include interaction with the KETs, Future and Emerging Technologies and Industrial Leadership pillars. There needs to be an effective means to search progress being made across H2020 projects, both during and after their execution, to facilitate dialogue that will lead to integration and incorporation of successful underpinning research into market oriented developments.

The success and even the survival of the EU industrial and technical basis depends on the success of the innovations reaching the market and on the social acceptance of the products for the EU citizen. This is the condition for a more resilient Europe. In order to benefit from best practices from third countries and to develop research and innovation allowing to address a more global situation and market, opportunities for international cooperation must be addressed at different levels: from the “doctrines” to the international standards. This should be conducted in a perspective of reciprocity.

**APPENDIX 1**

# Strategic vision for Secure Societies Research

*This strategic vision was a working paper prepared by a working group under the SSAG as a context for further analysis. It represents a set of key points against which more specific strategic planning should be tested.*

## 1. Strategic guidance covering period 2016-2020

- Identify lessons learned from FP7 (security research and cybersecurity research) and ongoing research in H2020: "mapping" of the main results in order to have the current state of the art and identify the main gaps and TRL for future research in H2020.

- Analyse main missions and related policies to highlight the key objectives achievable in the timeframe.

- Support market pull by a user-centred approach where solutions designed meet the needs and requirements of the users by consulting user groups and relevant stakeholders

- Implement a sequencing of projects: some kind of programme or clustering

- Set up monitoring and assessment system for verifying project delivery (against the roadmap and strategy), and link with other societal challenges

## 2. Strategic view to the topics of the Work Programmes

- two drivers: policies and market (both driven by the views of the users, including their funding capabilities). This covers both public and private sector applications

- consistency with security policies at EU level and Member State level : need for analysis of national policies, stakeholders and decision-making processes

- need to meet the user needs: requires detailed definition of needs and structured assessment of added value of solutions provided by research. S

- need to develop industry and SMEs competitiveness

- need to improve synergies and research efficiency between academics and industry

- need to identify spin-off effects benefitting other economic areas, and spin-in effects from technological developments elsewhere

## 3. Close-to-market research

The research and its requirements needs to be driven in a very dynamic way by emerging and evolving threat agents. The research needs to be able to respond flexibly to upcoming needs, and to public reactions to events. Requirements for security research are also driven by new technologies, such as cloud, and by social phenomena.
The innovation process in the security field differs from other fields in so far that big parts of the market are strongly regulated and the added value of new security solutions is difficult to be assessed by potential procurers. Both factors act as strong inertia to innovation. While innovation inhibited by regulation can be facilitated, or in some cases boosted, by adjusting regulations through decision makers, the assessment of the added value of new solutions can be improved by R&D activities themselves.

- WHAT?
  Broadly defined topics
  - Urban Security
  - Organized Crime (Europol Socta priorities)
  - Crime Prevention and 'petty, everyday crime'

  describe solution architectures per topic

- HOW?
  Research and innovation steps

  - Main market challenges:

    What are the market requirements (demand side) forecasts for industry sector products for the required time frame – short, medium and long?

    What are the implications of the market requirements on the industry sector products (supply side) in the short, medium and long term?

    What are industry's solutions to generate a market (dialogue with future customers or good knowledge): concrete innovations?

    The relationship between the 'user' of the technology and the purchaser needs to be explored and defined, including IPR issues. Governments have an important role to play in terms of support for industry standards. Product/technology development timescales also need to be considered.

    The market must be addressed in the mid to long term: by main categories of customers with their funding capabilities (for example several 10k€ or several 10 M€) and possible new instruments

  - Objectives across the different TRLs

  - Underpinning R&T or research at components level
    Screen existing results

Scout new, promising technologies
Identify key/critical technologies and technologies that may disappear from the EU supply chain

- Innovation and pilots
  Focus market-driven innovations- understand market opportunities
  Develop markets by policy-making
  Develop markets by disruptive innovations
  Develop common technologies between civil and military applications where possible
  Affordability, cost reduction and procurement instruments
  Opportunities for the export market
  pre-normative research

- Test and validation, certification
  Far-reaching adjustment of standardized solutions for individual implementation of solution

- WHO?
  Stakeholders :
  establish stable dialogue between different stakeholders to get consistent view on market needs, existing technology and industry capabilities

  - End-users
    creation of a platform with an enlarged panel of users
    stronger end-user involvement into the development of methods for validation and assessment and testing and into the assessment and testing

  - Buyers/procurers
    assess the market and main procedures – new procurement instrument is essential

  - SMEs
    find ways to integrate the innovation power of SMEs
    improve the bridge SME-industry-market: SMEs want to get attached to larger groups to minimize their efforts ad to have quick and confidential procedures and enlarge their geographical market

  - Industry
    Build on "champions" to create a strong supply chain'
    For cybersecurity: help create European champions
    Possibility to have several consortia, preferably smaller in parallel to test different solutions in innovation actions and actions closer to the market
    Consider instruments to support risk-taking
    Platforms per mission

  - Civil-military stakeholders
    Encourage synergies of solutions and uses between civil and military users, in

projects, especially in innovation actions
Map EDA and other MoDs projects of relevance in terms of technologies/applications for civil applications

## 4. Processes and instruments

- Need for shorter-term, flexible funding addressing real threats
- Innovation actions/Technology testbeds and incubators/Demo activities
  Security solutions with need for added value in many potential scenarios: iterative testing and participatory development of novel solutions under varying conditions and control of variables is needed; it refines solutions. Additional research activities are needed to eventually operationalize a solution.
  Requirement of quantified business and market impacts
- Pre-Commercial Procurement
  mechanism to canalize requirements, operationalize solutions and bring closer to a joint procurement by different member states
  seek solution for moving from a phase 1 to phase 2 (phase 2 call with several prototypes developed in parallel, co-funded by consortia of member states)
  provide incentive for member states to join efforts and build consortia for next phases
- PPI
- Fast track to innovation
  needs to be a flexible, quick, concrete instrument restricted to key players.
- CSA
  role of CSA: strategic research planning to support process of validation and assessment by providing data needed to assess the added value of solutions that is related to non-technical requirements such as organizational structures, policies, legal aspects.
  need for anthropological studies and other forms of research to better understand user needs and requirements, and help generate new opportunities for innovation
- IPR
  Ensure that project results can be used by end-users

## 5. The relationship between short, mid and long-term solutions

- need to align market introduction of innovations (products and services) with a typical duration of a call – 2 years

- test a programme or cluster approach that can address short term, simplified solutions, and then longer term solutions in a sequence
- longer term: more innovations, and growing TRLs and size in an overall sequence BUT focus should not be on long term as needs may change before they are implemented.

## 6. Link to deployment

Next to large-scale crime, everyday crime should be addressed. The Secure Societies programme should tap more into the market for services, products and environments to prevent crime.

Need to clearly and accurately define the term 'technology '. A broader definition may be appropriate

**APPENDIX 2**

# FTI – Fast Track to Innovation

*This proposal was prepared by a working group under the SSAG to set out recommended criteria for the Fast Track Innovation instrument. The SSAG consider this as of special importance to the Secure Societies area because of the dynamic nature of threats and security needs require an ability to initiate research and innovation in a way that is responsive to needs of users.*

## 1. Introduction and background

During the negotiations on Horizon 2020 programme, the European Parliament ensured that a novel instrument called "Fast Track to Innovation" (FTI) will be introduced in order to respond to the two most common complaints about FP7:

- Long time from idea to grant
- Too little room for bottom-up ideas

Considering these premises, the 'Fast Track to Innovation' instrument (FTI) has been designed to promote research and innovation with a focus on value creation and accelerate the development of technologies into innovative products, processes and services. Besides, FTI is aimed to speed up the time from idea to market and to increase the participation of private sector (industry, SMEs and first time applicants).

The implementation has been substantiated in the Rule for Participant art.54:

> *1. In accordance with Article 7, any legal entity may participate in a Fast Track to Innovation ("FTI") action. Actions funded under FTI shall be innovation actions. The FTI call shall be open to proposals relating to any technology field under the specific objective "Leadership in enabling and industrial technologies" set out in point 1 of Part II of Annex I to Regulation (EU) No 1291/2013 or to any of the specific objectives under the priority "Societal challenges" set out in points 1 to 7 of Part III of Annex I to that Regulation.*
>
> *2. Proposals may be submitted at any time. The Commission shall set three cut-off dates per year to evaluate proposals. The period between a cut-off date and signature of the grant agreement or notification of the grant decision shall not exceed six months. Proposals shall be ranked according to the impact, quality and efficiency of implementation and excellence, with the criterion of impact given a higher weighting.* Any legal entity will be eligible for application *and no more than five legal entities shall participate in any one action. The amount of the grant shall not exceed EUR 3 million.*

This scheme, which should be tested in form of pilots, will involve open calls with a bottom-up driven approach: participants from any sector could submit at any time a R&I project.

The procedure should target the three main objective of the commission:

- shorten the time to grant EU money, (max 6 months)
- allow smaller consortia to speed up time from idea to market (max 5 partners)

- increase participation of first-time applicants.

It will seek to stimulate private sector investment, promote research and innovation with a focus on value creation and accelerate the development of technologies into innovative products, processes and services.
Other similar action were already tested in FP6 with NEST[3] (New and Emerging Science and Technology) but was devoted in particular to SME and in Horizon 2020 with Future and Emerging Technologies Open Scheme (FET-OPEN[4]) but devoted to base research initiatives.

## 2. Description of the instrument

Activities shall cover the whole innovation cycle, but should focus on innovation-related activities, experimental and pre-commercial development, comprising the development stages from technology demonstration up to market uptake, including piloting, demonstration, test-beds, pre-normative research and standard setting, and market uptake of innovations. The aim of the proposal can deal with either "basic" technologies, or with applications (generic for multi-use) can provide a breakthrough by the use or the integration of other technologies/sciences (reaching a TRL closer to the market: above TRL 6, more TRL 7-8).

While being open to innovative ideas from all participants, the instrument is expected to increase industry participation in particular, since it have been primarily innovative industry (including SME) stakeholders that have repeatedly called for fast-track procedures in the past, highlighting the time-constraints they are facing in a highly competitive innovation-based global economy. Providing an actual instrument tailored to the needs of research-based companies is expected to increase the total number of proposals from industry participants as well as the total number of industry-driven projects eventually funded under Horizon 2020, thereby stimulating private investment in RDI and increasing the leverage effect of Horizon 2020.

## 3. Model Proposal

### a) Boundaries of the instrument

The Art. 54 RfP put specific boundaries to the instrument:

- Entities and consortiums
  - any legal entity
  - minimum 3, maximum 5 in consortium
- Grant

[3] NEST was a new activity in the Sixth Framework Programme (FP6). It aimed to support unconventional and visionary research with the potential to open new fields for European science and technology, as well as research on potential problems uncovered by science. There were no restrictions on the scientific fields to be addressed except that the research carried out under NEST should cut across or lie outside the thematic priority areas.

[4] FET-Open is a light, topic-agnostic and deadline free research funding scheme specifically designed to be open and continuously responsive to novel and fragile ideas that challenge current thinking, whenever they arise and wherever they come from.

  - maximum €3 million (up to 70% of funding), typically no more than €1 million grant
  - time-to-grant 6 months maximum
- Call and evaluation
  - always-open call — 3 cut-offs per year — no comitology
  - 'impact' higher weighting than 'quality' and 'efficiency

### b) Model Characteristics:

The model proposed has the following characteristics:

- Product idea originates in a company, according to end users requirements, and a company should lead the consortium,
- It intends to collaborate with international partners, e.g. other companies, RTOs or universities, to develop the product,
- The action should be structured according to a phase approach considering a feasibility study, R&D activities involving Businesses and Experimental Development Feasibility.
- Activities should be focused on Innovation and they should fulfil the following requirements: Besides there are additional requirements:
  - Creation of value.
  - Business innovation plan with clear milestones to achieve the innovation target.
  - Technology readiness level,
  - Time to market introduction.
- The focus of the instrument should be on commercialisation and impact:
  - Simplified business plan must be part of the proposal and they must commit a time-to-market of 1 to 2 years
- Consortia composition:
  - Business driven consortia,
  - Around 60% absorbed by companies,
  - Around 40% absorbed by RTOs or other non-industry partners,
  - minimum number of industry participants must be 2 in a consortium of 3 partners, and 3 in a consortium of 4 or 5.
- Budget in 2014-2015 WP
  - An agreement among R&I DGs has defined a budget for the pilot line: €100 mn
- taxed pro-rata across LEITs / SCs → Security 2.2% (over 60.60 % of LEIT–SC) → 3.6 M€ (2 project in 2015-2016)

- Duration of the projects
  - quick: 18 months to 2 years max, if not the innovation is already over, as it must be added to 4 + 6 Months maximum for delivering the proposal and been evaluated.

## 4. Recommendations for the implementation

### a) Coordination of calls:

There is a proposal to delegate all FTI budget lines to EASME (Executive Agency Small and Medium Enterprise).

We recommend giving the coordination to the DG already coordinating the different themes. For Secure Societies: DG ENTR/REA.

**b) Topics:**

- The instrument should be open with a bottom-up approach but the topic of a proposal should relate to one of the four main streams (DRS, BES, FCT and DS) from the current work programme.

**c) Synchronization (or not) with the present calls schedule**

- permanent open call, with 3 evaluation per year (1 synchronized with normal call)

**d) Submission forms:**

- Single-stage application process, but the application may be in two parts,
- Little bureaucracy and simple forms.

**e) Evaluation:**

- To have 6 months' time-to-grant we propose to keep "one stage" evaluation process.
- Evaluation criteria to focus on excellence in innovation, commercialisation potential, economic impact and the company's potential achieving the envisaged results.
- "Impact" criterion given a higher weighting in evaluations (for example 2.0 instead of 1.5 as it is for innovation action) and having a threshold at 4 and not 3 as it is normal.
- one of the requirements is to have a real test bed and users of the product providing input throughout the development processes.
- Evaluation by experts representing the market and having a business understanding (users, industry itself, etc). Indeed, strong weight on the impact criterion with a measurable innovation perspective.
- Evaluations can be carried out in different fashions (web-based rather than on-site, introduction of an abstract-oriented first stage selection) without compromising on quality.
- The publication of the results will be immediate after the evaluation process.

**f) Budget:**

- Higher levels of funding for the closer projects to market – aids demonstration and scale up
- For the pilot phase is correct to have small budget (6 M€) but a greater budget should be dedicated in future calls.